doi: 10.14232/actasm-015-259-3

Acta Sci. Math. (Szeged)
81 (2015), 643–683

Geometric constructibility of cyclic polygons and a limit theorem

GÁBOR CZÉDLI and ÁDÁM KUNOS

Dedicated to the eightieth birthday of Professor László Leindler

Communicated by Á. Kurusa

Abstract. We study *convex cyclic polygons*, that is, inscribed n-gons. Starting from P. Schreiber's idea, published in 1993, we prove that these polygons are not constructible from their *side lengths* with straightedge and compass, provided n is at least five. They are non-constructible even in the particular case where they only have *two* different *integer* side lengths, provided that $n \neq 6$. To achieve this goal, we develop two tools of separate interest. First, we prove a *limit theorem* stating that, under reasonable conditions, geometric constructibility is preserved under taking limits. To do so, we tailor a particular case of Puiseux's classical theorem on some generalized power series, called *Puiseux series*, over algebraically closed fields to an analogous theorem on these series over real square root closed fields. Second, based on *Hilbert's irreducibility theorem*, we give a *rational parameter theorem* that, under reasonable conditions again, turns a non-constructibility result with a transcendental parameter into a non-constructibility result with a rational parameter. For n even and at least six, we give an elementary proof for the non-constructibility of the cyclic n-gon from its side lengths and, also, from the *distances* of its sides from the center of the circumscribed circle. The fact that the cyclic n-gon is constructible from these distances for $n = 4$ but non-constructible for $n = 3$ exemplifies that some conditions of the limit theorem cannot be omitted.

Received February 13, 2015.
AMS Subject Classifications: 51M04, 12D05.
Key words and phrases: inscribed polygon, cyclic polygon, circumscribed polygon, compass and ruler, straightedge and compass, geometric constructibility, Puiseux series, power series, holomorphic function, field extension, Hilbert's irreducibility theorem.
This research was supported by the European Union and co-funded by the European Social Fund under the project "Telemedicine-focused research activities on the field of Mathematics, Informatics and Medical sciences" of project number "TÁMOP-4.2.2.A-11/1/KONV-2012-0073", and by NFSR of Hungary (OTKA), grant number K83219.

1. Introduction

1.1. Target and some of the results

A *cyclic polygon* is a convex n-gon inscribed in a circle. Here n denotes the *order*, that is the number of vertices, of the polygon. *Constructibility* is always understood as the classical geometric constructibility with straightedge and compass. Following Dummit and Foote [4, bottom of page 534], we speak of an (unruled) *straightedge* rather than a *ruler*, because a ruler can have marks on it that we do not allow. We know from Schreiber [25, proof of Theorem 2] that

> There exist positive real numbers a, b, c such that the cyclic pentagon with side lengths a, a, b, b, c exists but it is not constructible from a, b, c with straightedge and compass. (1.1)

Oddly enough, the starting point of our research was that we could not understand the proof of Schreiber's next statement, [25, Theorem 3], which says that

> If $n > 5$, then the cyclic n-gon is in general not constructible from its side lengths with straightedge and compass. (1.2)

We analyze the meaning of "in general not constructible" later in the paper. Supported by the details given in the present paper later, we think that the proof of (1.2) given in [25] is incomplete. Fortunately, one can complete it with the help of our limit theorem, Theorem 9.1, which is of separate interest. Furthermore, the limit theorem leads to a slightly stronger statement.

We are only interested in the constructibility of a *point* depending on finitely many given points, because the constructibility of many other geometric objects, including cyclic polygons, reduces to this case easily. A *constructibility program* is a finite list of instructions that concretely prescribe which elementary Euclidean step for which points should be performed to obtain the next point. For example,

> "Take the intersection of the line through the ninth and the thirteenth points with the circle whose center and radius are the first point and the distance between the fourth and sixth points, respectively." (1.3)

can be such an instruction. This instruction is not always meaningful (e.g., the ninth and the thirteenth points may coincide and then they do not determine a line) and it can allow choices (which intersection point should we choose). If there is a "good" choice at each instruction such that the last instruction produces the point that we intend to construct, then the constructibility program *works* for the given data, that is, for the initial points. In our statements below, unless concrete data are mentioned,

$$\text{A positive statement of \textit{constructibility} means the existence of a constructibility program that works \textit{for all meaningful data}, that is, for data defining a non-degenerate cyclic polygon of the given order.} \tag{1.4}$$

The cyclic polygon with side lengths $a_1, \dots, a_n$, in this order, is denoted by $P_n(a_1, \dots, a_n)$. As usual, $\mathbb{N} := \{1, 2, 3, \dots\}$ and $\mathbb{N}_0 := \{0\} \cup \mathbb{N}$. For $i \in \mathbb{N}$, we define

$$\begin{aligned} \mathrm{NCL}(i) = \big\{ n \in \mathbb{N} : \exists \langle a_1, \dots, a_n \rangle \in \mathbb{N}^n &\text{ such that } P_n(a_1, \dots, a_n) \\ &\text{exists, it is not constructible from } a_1, \dots, a_n, \text{ and} \\ &|\{a_1, \dots, a_n\}| \le i \big\}; \end{aligned} \tag{1.5}$$

the acronym comes from "Non-Constructible from side Lengths". Note that the Gauss–Wantzel theorem, see Wantzel [27], can be formulated in terms of NCL(1); for example, $7 \in \mathrm{NCL}(1)$ and $17 \notin \mathrm{NCL}(1)$. More precisely, $n \in \mathrm{NCL}(1)$ iff the regular cyclic n-gon is non-constructible iff n is not of the form $2^k p_1 \cdots p_t$ where $k, t \in \mathbb{N}_0$ and $p_1, \dots, p_t$ are pairwise distinct Fermat primes. If n belongs to $\mathrm{NCL}(i)$ for some $i \in \mathbb{N}$, then the cyclic n-gon is not constructible in our sense given in (1.4) or in any reasonable "general" sense. Clearly, for $i = 1$, $\mathbb{N}^n$ in (1.5) can be replaced by $\mathbb{R}^n$, because the unit distance at a geometric construction is up to our choice. However, for $i > 1$, $\mathbb{N}^n$ in (1.5) rather than $\mathbb{R}^n$ makes Theorem 1.1 below stronger. One of our goals is to prove the following theorem, which is a stronger statement than (1.2). Parts (iii) and (iv) below can be combined; however, we formulate them separately, because we have an elementary proof for (iii) but not for (iv). Part (c) is well known.

Theorem 1.1.

(i) *For $n \in \{3, 4\}$, the cyclic n-gon is constructible in general from its side lengths with straightedge and compass.*

(ii) (a) $5 \in \mathrm{NCL}(2) \setminus \mathrm{NCL}(1)$.

(b) $6 \in \mathrm{NCL}(3)$ *but* $6 \notin \mathrm{NCL}(2)$. *Furthermore, if $a_1, \dots, a_6$ are positive* real *numbers such that $P_6(a_1, \dots, a_6)$ exists and $|\{a_1, \dots, a_6\}| \le 2$, then the cyclic hexagon $P_6(a_1, \dots, a_6)$ can be constructed from its side lengths.*

(c) $7 \in \mathrm{NCL}(1)$.

(iii) *If $n \ge 8$ is an* even *integer, then $n \in \mathrm{NCL}(2)$.*

(iv) *If $n \ge 8$ is an* odd *integer, then $n \in \mathrm{NCL}(2)$.*

Note that if the regular n-gon is non-constructible, then $n \in \mathrm{NCL}(1)$. However, if the regular n-gon is constructible, and infinitely many $n \ge 8$ are such, then $n \notin \mathrm{NCL}(1)$ and, for these n, parts (iii) and (iv) above cannot be strengthened by changing NCL(2) to NCL(1). The elementary method we use to prove Part (iii) of Theorem 1.1 easily leads us to the following statement on cyclic n-gons of *even order*; see Figure 1.1 for an illustration.

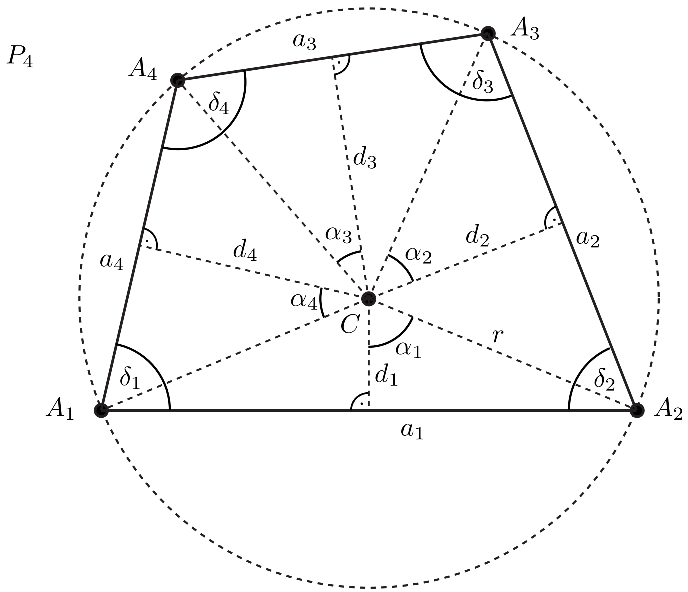

Figure 1.1. A cyclic n-gon for $n = 4$

Assume that, with straightedge and compass, we want to construct the cyclic n-gon $D_n(d_1, \dots, d_n)$ from the distances $d_1, \dots, d_n$ of its sides from the center of its circumscribed circle. We define NCD(i) analogously to (1.5); now the acronym comes from 'Non-Constructible from Distances".

Theorem 1.2. *If $n \geq 6$ is even, then $n \in \mathrm{NCD}(2)$.*

Evidently, $n \in \mathrm{NCD}(1)$ iff the regular n-gon is non-constructible. To shed more light on Theorem 1.2, we recall the following statement from Czédli and Szendrei [3, IX.1.26–27,2.13 and page 309], which was proved by computer algebra.

Proposition 1.3. ([3]) *Let $A_4 := \{6, 8\}$, $A_3 := \{3, 5, 12, 24, 30\}$,*

$$A_2 := \{10, 15, 16, 17, 20, 32, 34, 40, 48, 51, 60, 64, 68, 80, 85, 96\},$$

and $A_1 := \{3, 5, 6, 7, \dots, 100\} \setminus (A_2 \cup A_3 \cup A_4)$. Then, for every $i \in \{1, 2, 3, 4\}$, $A_i \subseteq \mathrm{NCD}(i)$. As opposed to $D_3(d_1, \dots, d_3)$, $D_4(d_1, \dots, d_4)$ is constructible from $\langle d_1, \dots, d_4 \rangle$.

Note that we do not claim that $A_i \cap \mathrm{NCD}(i-1) = \emptyset$. The following statement, which we recall from Czédli and Szendrei [3, IX.2.14], extends the scope of Theorem 1.2 to circumscribed polygons.

Remark 1.4. ([3]) Let $3 \le n \in \mathbb{N}$. With the notation given before Theorem 1.2, a circumscribed n-gon T_n is constructible from the distances $t_1, \dots, t_n$ of its vertices from the center of the inscribed circle if and only if the inscribed polygon $D_n(1/t_1, \dots, 1/t_n)$ is constructible from $\langle 1/t_1, \dots, 1/t_n \rangle$ or, equivalently, from $\langle t_1, \dots, t_n \rangle$.

1.2. Prerequisites and outline

Undergraduate, or sometimes graduate, mathematics is sufficient to follow the paper. The reader is assumed to know the rudiments of simple field extensions and that of calculus. Following, say, Cohn [1, page 9], Grätzer [8, page 1], and Rédei [26, page 12], the notation $X \subset Y$ stands for proper inclusion, that is, $X \subset Y$ iff $X \subseteq Y$ and $X \neq Y$.

The paper is structured as follows. Section 2 gives Schreiber's argument for (1.2). Section 3 gives an elementary proof for part (iii) of Theorem 1.1, that is, for all even $n \ge 8$; this section also proves Theorem 1.2 for $n \ge 8$. Section 4 is devoted to cyclic polygons of small order, that is, for $n < 8$; here we prove parts (i)–(ii) of Theorem 1.1 and the case $n = 6$ of Theorem 1.2. Also, this section recalls some arguments from [3] to prove some parts of Proposition 1.3. In Section 5, we comment on Schreiber's argument. Section 6 collects some basic facts on field extensions. In particular, this section gives a rigorous algebraic treatment for real functions composed from the four arithmetic operations and $\sqrt{}$. Section 7 proves that the functions from the preceding section can be expanded into *power series with dyadic rational exponents* such that the coefficients of these series are geometrically constructible. Section 8 compares these expansions with Puiseux series and Puiseux's theorem. Based on our expansions from Section 7, we prove a *limit theorem* for geometric constructibility in Section 9. Using this theorem, Section 10 proves a weaker form of parts (iii)–(iv) of Theorem 1.1, with transcendental parameters rather than integer ones, and points out how one could complete Schreiber's argument. Armed with Hilbert's irreducibility theorem, Section 11 proves a *rational parameter theorem* that, under reasonable conditions, turns a non-constructibility result with a transcendental parameter into a non-constructibility result with a rational parameter. Finally, based on the tools elaborated in the earlier sections, Section 12 completes the proof of Theorem 1.1 only in few lines.

Since the Limit Theorem and the Rational Parameter Theorem are about geometric constructibility in general, not only for cyclic polygons, they can be of separate interest.

2. Schreiber's argument

Most of Schreiber [25] is clear and practically all mathematicians can follow it. We only deal with [25, page 199, lines 3–15], where, in order to prove (1.2), he claims to perform the induction step from $(n-1)$-gons to n-gons. His argument is basically the following paragraph; the only difference is that we use the radius (of the circumscribed circle) rather than the coordinates of the vertices. This simplification is not an essential change, because the (geometric) constructibility of a cyclic n-gon is clearly equivalent to the constructibility of its radius.

Suppose, for a contradiction, that the radius of the cyclic n-gon is in general constructible from the side lengths $a_1, \dots, a_n$. Hence, this radius is a quadratic irrationality R depending on the variables $a_1, \dots, a_n$, and such as it is a continuous function of its n variables. On the other hand, the geometric dependence of the radius from $a_1, \dots, a_n$ is described by a continuous function f of the same variables. Because for $a_n \to 0$ the radius of the n-sided inscribed polygon converges to that of the $(n-1)$-sided polygon with side lengths $a_1, \dots, a_{n-1}$ and the continuous functions R and f are identical for $a_n \neq 0$, R takes the same limit value for $a_n \to 0$ as f. That is, for $a_n = 0$, the quadratic irrationality R describes the constructibility of the radius of the inscribed $(n-1)$-gon. Finally, iterating the same process, we obtain that the radius of the cyclic $(n-2)$-gon, that of the cyclic $(n-3)$-gon, ..., that of the cyclic 5-gon are constructible, which contradicts (1.1).

Schreiber's argument will be analyzed in Section 5.

3. An elementary proof for n even

Let $a_1, \dots, a_n$ be arbitrary positive real numbers. It is proved in Schreiber [25, Theorem 1] that

$$\begin{array}{l}\text{There exists a cyclic } n\text{-gon with side lengths } a_1, \dots, a_n \\ \text{iff } a_j < \sum\{a_i : i \neq j\} \text{ holds for every } i \in \{1, \dots, n\}.\end{array} \tag{3.1}$$

Our elementary approach will be based on the following well-known statement from classical algebra. Unfortunately, a thorough treatment of geometric constructibility is usually missing from current books on algebra in English, at least in our reach; so it is not so easy to give references. Part (A) below is Herstein [9, Theorem 5.5.2 in page 206] and [3, Theorem III.3.1 in page 63]. Part (B) is the well-known Eisenstein-Schönemann criterion, see Cox [2] for our terminology. Part (C) is less elementary and will only be used in Section 11, but even this part is often taught for graduate students. This part is [3, Theorem V.3.6], and also Kiss [14, Theorem 6.8.17], Kersten [13, Satz in page 158], and Jacobson [12, Criterion 4.11.B in page 263]. It also follows from Gilbert and Nicholson [7, Theorem 13.5 in page 254] (combined with Galois theory). The degree of a polynomial $f = f(x)$ is denoted by $\deg(f)$, or by $\deg_x(f)$ if we want to indicate the variable. Let $a_1, \dots, a_k$, and b be real numbers; as usual, the smallest subfield K of $\mathbb{R}$ such that $\{a_1, \dots, a_k\} \subseteq K$ is denoted by $\mathbb{Q}(a_1, \dots, a_n)$. In this case, instead of "b is constructible from $a_1, \dots, a_k$", we can also say that b is *constructible over* the field K. We shall use this terminology only for finitely generated subfields of $\mathbb{R}$. By definition, a *complex number is constructible* if both of its real part and imaginary part are constructible. Equivalently, if it is constructible as a point of the plane.

Proposition 3.1.

(A) *If $f \in \mathbb{Q}[x]$ is an irreducible polynomial in $\mathbb{Q}[x]$, $c \in \mathbb{R}$, $f(c) = 0$, and the degree* $\deg(f)$ *is not a power of 2, then c is not constructible over $\mathbb{Q}$.*

(B) *If $f(x) = \sum_{j=0}^{k} a_j x^j \in \mathbb{Z}[x]$ and p is a prime number such that $p \nmid a_k$, $p^2 \nmid a_0$, and $p \mid a_j$ for $j \in \{0, \dots, k-1\}$, then $f(x)$ is irreducible in $\mathbb{Q}[x]$.*

(C) *Let K be a finitely generated subfield of $\mathbb{R}$. If $f \in K[x]$ is an irreducible polynomial in $K[x]$, $c \in \mathbb{R}$, and $f(c) = 0$, then c is constructible over K if and only if the degree of the splitting field of f over K is a power of 2.*

For $k \in \mathbb{N}$, we need the following two known formulas, which are easily derived from de Moivre's formula and the binomial theorem. For brevity, the conjunction of "$2 \mid j$" and "j runs from 0" is denoted by $2 \mid j = 0$, while $2 \nmid j = 1$ is understood analogously.

$$\sin(k\gamma) = \sum_{2 \nmid j=1}^{k} (-1)^{(j-1)/2} \binom{k}{j} (\cos\gamma)^{k-j} \cdot (\sin\gamma)^j, \tag{3.2}$$

$$\cos(k\gamma) = \sum_{2 \mid j=0}^{k} (-1)^{j/2} \binom{k}{j} (\cos\gamma)^{k-j} \cdot (\sin\gamma)^j. \tag{3.3}$$

A prime p is a *Fermat prime*, if $p - 1$ is a power of 2. A Fermat prime is necessarily of the form $p_k = 2^{2^k} + 1$. We know that $p_0 = 3$, $p_1 = 5$, $p_2 = 17$, $p_3 = 257$, and $p_4 = 65\,537$ are Fermat primes, but it is an open problem if there exists another Fermat prime.

Lemma 3.2. *If $8 \le n \in \mathbb{N}$, then there exists a prime p such that $n/2 < p < n$ and p is not a Fermat prime.*

Proof. We know from Nagura [16] that, for each $25 \le x \in \mathbb{R}$, there exists a prime in the open interval $(x, 6x/5)$. Applying this result twice, we obtain two distinct primes in $(x, 36x/25)$. Hence, for $50 \le n \in \mathbb{N}$, there are at least two primes in the interval $(n/2, n)$. Since the ratio of two consecutive Fermat primes above 25 is more than 2, this gives the lemma for $50 \le n$. For $8 \le n \le 50$, appropriate primes are given in the following table.

n	8–13	14–25	26–45	46–85
p	7	13	23	43

■

Proof of Theorem 1.1 (iii). Let $n \ge 8$ be even. It suffices to find an appropriate p in the set $\{1, 2, \dots, n-1\}$ and $a, b \in \mathbb{N}$ such that P_n is not constructible even if p of the given n side lengths are equal to a and the rest $n-p$ side lengths are equal to b, for appropriate integers a and b. Let r and C be the radius and the center of the circumscribed circle, respectively.

The half of the central angle for a and b are denoted by α and β, respectively; see the α_i in Figure 1.1 for the meaning of half central angles. Clearly, P_n is constructible iff so is $u = 1/(2r)$. Since we will choose a and b nearly equal, C is in the interior of P_n, and we have

$$p\alpha + (n-p)\beta = \pi. \tag{3.4}$$

It follows from (3.4) that $\sin(p\alpha) - \sin((n-p)\beta) = 0$. Therefore, using (3.2),

$$\sin\alpha = au,\ \sin\beta = bu,\ \cos\alpha = \sqrt{1-a^2u^2},\ \text{and}\ \cos\beta = \sqrt{1-b^2u^2}, \tag{3.5}$$

we obtain that u is a root of the following function:

$$\begin{aligned} f_p^{(1)}(x) = &\sum_{2\nmid j=1}^{p} (-1)^{(j-1)/2}\binom{p}{j}(1-a^2x^2)^{(p-j)/2}\cdot(ax)^j - \\ &- \sum_{2\nmid j=1}^{n-p} (-1)^{(j-1)/2}\binom{n-p}{j}(1-b^2x^2)^{(n-p-j)/2}\cdot(bx)^j \\ = &\ \Sigma_1^f - \Sigma_2^f. \end{aligned} \tag{3.6}$$

Observe that $f_p^{(1)}(x)$ is a polynomial since $p-j$ and $n-p-j$ are even for j odd. In fact, $f_p^{(1)}(x) \in \mathbb{Z}[x]$ for all $a, b \in \mathbb{N}$. Besides $f_p^{(1)}(x) = \Sigma_1^f - \Sigma_2^f$, we also consider the polynomial $f_p^{(2)}(x) = \Sigma_1^f + \Sigma_2^f$.

From now on, we assume that

$$8 \le n \text{ is even and } p \text{ is chosen according to Lemma 3.2.} \tag{3.7}$$

It is obvious by (3.1) that we can choose positive integers a and b such that

$$a \equiv 1 \pmod{p^2}, \quad b \equiv 0 \pmod{p^2}, \tag{3.8}$$

and a/b is so close to 1 that P_n exists and C is in the interior of P_n. The inner position of C is convenient but not essential, because we can allow a central angle larger than π; then (3.5) still holds and the sum of half central angles is still π.

Let $v \in \{1, 2\}$. The assumption $n/2 < p < n$ gives $\deg_x(f_p^{(v)}) = p$. Hence, we can write

$$f_p^{(v)}(x) = \sum_{s=0}^{p} c_s^{(v)} x^s, \quad \text{where } c_0^{(v)}, \dots, c_p^{(v)} \in \mathbb{Z}.$$

We have $c_0^{(v)} = 0$ since $j > 0$ in (3.6). Our plan is to apply Proposition 3.1(B) to the polynomial $f_p^{(v)}(x)/x$. Hence, we are only interested in the coefficients $c_s^{(v)}$ modulo p^2. Note that this congruence extends to the polynomial ring $\mathbb{Z}[x]$ in the usual way. The presence of $(bx)^j$ in Σ_2^f yields that all coefficients in Σ_2^f are congruent to 0 modulo p^2. Therefore, $f_p^{(v)}(x) \equiv \Sigma_1^f \pmod{p^2}$, and we can assume that all the $c_s^{(v)}$ come from Σ_1^f. Each summand of Σ_1^f is of degree p. Therefore, computing modulo p^2, the leading coefficient $c_p^{(v)}$ satisfies the following:

$$\begin{aligned} c_p^{(v)} &\equiv \sum_{2 \nmid j=1}^{p} (-1)^{(j-1)/2} \binom{p}{j} (-1)^{(p-j)/2} (a^2)^{(p-j)/2} a^j \\ &= (-1)^{(p-1)/2} \sum_{2 \nmid j=1}^{p} \binom{p}{j} a^p \equiv (-1)^{(p-1)/2} \sum_{2 \nmid j=1}^{p} \binom{p}{j} \\ &= (-1)^{(p-1)/2} 2^{p-1} = (-1)^{(p-1)/2} + pt_p \pmod{p^2} \quad \text{for some } t_p \in \mathbb{Z}; \end{aligned} \tag{3.9}$$

the last but one equality is well known while the last one follows from Fermat's little theorem. Since Σ_1^f gives a linear summand only for $j = 1$, we have

$$c_1^{(v)} \equiv \binom{p}{1} \cdot a = pa \equiv p \pmod{p^2}. \tag{3.10}$$

Next, let $1 \le s < p$. For $j = p$, the j-th summand of Σ_1^f is $\pm(ax)^p$, which cannot influence $c_s^{(v)}$. Hence, modulo p^2, $c_s^{(v)}$ comes from the $\sum_{2 \nmid j=1}^{p-2}$ part of Σ_1^f. However, for $j \in \{1, \dots, p-2\}$, the binomial coefficient $\binom{p}{j}$ is divisible by p. Hence, we conclude that there exist integers $t_1, \dots, t_{p-1}$ such that

$$c_s^{(v)} \equiv pt_s \pmod{p^2} \quad \text{for } s \in \{1, \dots, p-1\}. \tag{3.11}$$

Now, (3.9), (3.10), (3.11), $c_0^{(v)} = 0$, and Proposition 3.1(B) imply that

$$\text{for } v = 1, 2, \quad f_p^{(v)}(x)/x \text{ is irreducible.} \tag{3.12}$$

By the choice of p, $\deg_x(f_p^{(v)}(x)/x) = p - 1$ is not a power of 2. Since $a, b \in \mathbb{Z}$, we can apply Proposition 3.1(A) to $f_p^{(1)}(x)/x$ to conclude that P_n is not constructible. This proves Theorem 1.1 (iii). ∎

Proof of Theorem 1.2 for $n \geq 8$. Let p be a prime according to Lemma 3.2. Choose $a, b \in \mathbb{N}$ according to (3.8) such that a/b be sufficiently close to 1. Let $d_1 = \cdots = d_p = a$ and $d_{p+1} = \cdots = d_n = b$ be the distances of the sides of D_n from C. Hence, $D_n = D_n(a, \ldots, a, b, \ldots, b)$ exists and, clearly, its interior contains the center C of the circumscribed circle. (Note that the inner position of C is convenient but not essential if we allow that one of the given distances can be negative.) The radius of the circumscribed circle is denoted by r, and let $u = 1/r$. Instead of (3.5), now we have

$$\cos\alpha = au,\ \cos\beta = bu,\ \sin\alpha = \sqrt{1 - a^2u^2},\ \text{and}\ \sin\beta = \sqrt{1 - b^2u^2}. \tag{3.13}$$

Combining (3.3), (3.4), and (3.13), and using $2 \nmid p$ and $2 \nmid n - p$, we obtain that u is a root of the following polynomial:

$$\begin{aligned} g_p(x) = &\sum_{2|j=0}^{p-1} (-1)^{j/2} \binom{p}{j} (ax)^{p-j} (1 - a^2x^2)^{j/2} + \\ &+ \sum_{2|j=0}^{n-p-1} (-1)^{j/2} \binom{n-p}{j} (bx)^{n-p-j} (1 - b^2x^2)^{j/2} = \Sigma_1^g + \Sigma_2^g. \end{aligned} \tag{3.14}$$

Substituting s for $p - j$ in Σ_1^g above and using the rule $\binom{p}{j} = \binom{p}{p-j}$, we obtain $\Sigma_1^g = (-1)^{(p-1)/2} \cdot \Sigma_1^f$. Similarly, substituting s for $n - p - j$ in Σ_2^g, we obtain $\Sigma_2^g = (-1)^{(n-p-1)/2} \cdot \Sigma_2^f$. Hence, $\{g_p(x), -g_p(x)\} \cap \{f_p^{(1)}(x), f_p^{(2)}(x)\} \neq \emptyset$, and (3.12) yields that $g_p(x)/x$ is irreducible. Therefore, Proposition 3.1 implies that $D_n(a, \ldots, a, b, \ldots, b)$ is not constructible. This proves Theorem 1.2 for the case $2 \mid n \geq 8$. ∎

4. Cyclic polygons of small order

The ideas we use in this section are quite easy. However, the concrete computations often require and almost always make it reasonable to use computer algebra.

The corresponding Maple worksheet (Maple version V.3 of November 27, 1997) is available from the authors' web sites.

Definition 4.1. For $k, m \in \mathbb{N}$ and $a, b \in \mathbb{R}$, we define the following polynomials. (We will soon see that the mnemonic superscripts s and c come from sine and cosine; the first one refers to a single angle while the second one to a multiple angle. The superscripts 0 and 1 refer to the parity of the subscripts.)

$$\begin{aligned}
f_k^{\text{s-s}}(x) &:= \sum_{2 \nmid j=1}^{k} (-1)^{(j-1)/2} \binom{k}{j} (1-x^2)^{(k-j)/2} \cdot x^j, \quad \text{for } k \text{ odd},\\
f_k^{\text{s-c}}(x) &:= \sum_{2 \mid j=0}^{k} (-1)^{j/2} \binom{k}{j} (1-x^2)^{(k-j)/2} \cdot x^j, \quad \text{for } k \text{ even},\\
W_{k,m}^{11}(a,b,x) &:= f_k^{\text{s-s}}(ax) - f_m^{\text{s-s}}(bx), \ \text{for } k, m \text{ odd},\\
W_{k,m}^{00}(a,b,x) &:= f_k^{\text{s-c}}(ax) + f_m^{\text{s-c}}(bx), \ \text{for } k, m \text{ even},\\
W_{k,m}^{10}(a,b,x) &:= \left(f_k^{\text{s-s}}(ax)\right)^2 + \left(f_m^{\text{s-c}}(bx)\right)^2 - 1, \ \text{for } k \text{ odd and } m \text{ even},\\
W_{k,m}^{01}(a,b,x) &:= \left(f_k^{\text{s-c}}(ax)\right)^2 + \left(f_m^{\text{s-s}}(bx)\right)^2 - 1, \ \text{for } k \text{ even and } m \text{ odd},\\
W_{k,m}(a,b,x) &:= W_{k,m}^{i_k i_m}(a,b,x), \ \text{where } i_k \equiv k \text{ and } i_m \equiv m \pmod 2.
\end{aligned}$$

Lemma 4.2. *Let $k, m \in \mathbb{N}$ and $0 < a, b \in \mathbb{R}$.*

(i) *If k is odd, then $f_k^{\text{s-s}}(x) \in \mathbb{Z}[x]$ is a polynomial of degree k and, for $\alpha \in \mathbb{R}$, $f_k^{\text{s-s}}(\sin(\alpha)) = \sin(k\alpha)$. The leading coefficient of $f_k^{\text{s-s}}(x)$ is $(-1)^{(k-1)/2} \cdot 2^{k-1}$.*

(ii) *If k is even, then $f_k^{\text{s-c}}(x) \in \mathbb{Z}[x]$ is a polynomial of degree k and, for $\alpha \in \mathbb{R}$, $f_k^{\text{s-c}}(\sin(\alpha)) = \cos(k\alpha)$. The leading coefficient of $f_k^{\text{s-c}}(x)$ is $(-1)^{k/2} \cdot 2^{k-1}$.*

(iii) *$W_{k,m}(a,b,x)$ is a polynomial with indeterminate x. If the parameters a and b are also treated as indeterminates, then $W_{k,m}(a,b,x)$ is a polynomial over $\mathbb{Z}$. For $0 < a \in \mathbb{R}$ and $0 < b \in \mathbb{R}$, if $a \neq b$, or $k \neq m$, or $k = m$ is even, then $W_{k,m}(a,b,x)$ is not the zero polynomial. Furthermore, if the cyclic polygon*

$$P_n(\underbrace{a, \dots, a}_{k \text{ copies}}, \underbrace{b, \dots, b}_{m \text{ copies}}) \tag{4.1}$$

exists and r denotes the radius of its circumscribed circle, then we have that $W_{k,m}(a,b,1/(2r)) = 0$.

Proof. Since $0 = (1-1)^k = \sum_{j=0}^{k} (-1)^j \binom{k}{j}$ and $2^k = \sum_{j=0}^{k} \binom{k}{j}$,

$$\sum_{2 \nmid j=1}^{k} \binom{k}{j} = 2^{k-1} \quad \text{and} \quad \sum_{2 \mid j=0}^{k} \binom{k}{j} = 2^{k-1}.$$

We conclude easily from these equalities, (3.2), and (3.3) that parts (i) and (ii) of the lemma hold. These parts imply that $W_{k,m}(a,b,x)$ is a polynomial and, for positive real numbers a and b, it is the zero a polynomial iff $a=b$, $k=m$, and $k=m$ is odd. Let $u=1/(2r)$. Denoting the half of the central angle for a and b by α and β, as in the proof of Theorem 1.1 (iii), we obtain that $\sin(\alpha)=au$ and $\sin(\beta)=bu$. Let $\widehat{\alpha}=k\alpha$ and $\widehat{\beta}=m\beta$. Since $\widehat{\alpha}+\widehat{\beta}=\pi$, we have

$$\begin{gathered}\sin(\widehat{\alpha})=\sin(\widehat{\beta}),\quad \cos(\widehat{\alpha})=-\cos(\widehat{\beta}),\\ \big(\sin(\widehat{\alpha})\big)^2+\big(\cos(\widehat{\beta})\big)^2=1,\quad \big(\cos(\widehat{\alpha})\big)^2+\big(\sin(\widehat{\beta})\big)^2=1.\end{gathered}\tag{4.2}$$

Therefore, part (iii) follows easily from parts (i) and (ii) and 4.2. ■

Proof of Theorem 1.2 for $n=6$. We follow Czédli and Szendrei [3, IX.2.13]; only the values of the d_i are different. Let

$$d_1=d_2=d_3=d_4=1000,\ d_5=999, \text{ and } d_6=1001.\tag{4.3}$$

Using continuity, it is straightforward but tedious to show that $D_6(d_1,\dots,d_6)$ exists; the details are omitted. Let $\alpha_1,\dots,\alpha_6$ denote the central half angles. As usual, $\cos(\alpha_5)=d_5u=999u$, where $u=1/r$, and $\cos(\alpha_6)=d_6u=1001u$. We obtain from (3.3) and $\cos(\alpha_1)=d_1u=1000u$ that $\cos(\alpha_1+\dots+\alpha_4)=\cos(4\alpha_1)=8(\cos(\alpha_1))^4-8(\cos(\alpha_1))^2+1=8\cdot 10^{12}u-8\cdot 10^6u+1$. These equalities, (4.5), which we recall from [3] soon, and $4\alpha_1+\alpha_5+\alpha_6=\pi$ imply that u, which is not 0, is a root of a polynomial of degree 8 in $\mathbb{Z}[x]$. We easily obtain this polynomial by computer algebra. It is divisible by $4\,000\,000x^2$ and contains no summand of odd degree. Therefore, dividing the polynomial by $4\,000\,000x^2$, we obtain that u^2 is a root of

$$16\cdot 10^{18}\cdot x^3-28\,000\,004\cdot 10^6\cdot x^2+16\,000\,004\cdot x-3.$$

By computer algebra, this polynomial is irreducible. Hence u^2 is not constructible, implying that none of u, $r=1/u$, and $D_6(d_1,\dots,d_6)$ is constructible. This completes the proof of Theorem 1.2. ■

Proof of Theorem 1.1 (i) and (ii). Unless otherwise stated, we keep the notation from the proof of part (iii). In particular, $u=1/(2r)$. The case $n=3$ is trivial.

Assume $n=4$. With the notation of Figure 1.1 and using the fact that $\cos\delta_3=\cos(\pi-\delta_1)=-\cos\delta_1$, the law of cosines gives

$$a_1^2+a_3^2-2a_1a_3\cos\delta_1=\overline{A_2A_4}^{\,2}=a_2^2+a_4^2+2a_2a_4\cos\delta_1,\tag{4.4}$$

which yields an easy expression for $\cos\delta_1$. This implies that $\cos\delta_1$ is constructible, and so is the cyclic quadrangle P_4. This settles the case $n = 4$.

Next, let $n = 5$. Note that we know from Schreiber [25, Theorem 2 and its proof] that $5 \in \mathrm{NCL}(3)$; however, we intend to show that $5 \in \mathrm{NCL}(2)$. By (3.1), the cyclic pentagon $P_5(1, 2, 2, 2, 2)$ exists. By Lemma 4.2(iii), $u = 1/(2r)$ is a root of the polynomial $W_{1,4}(1, 2, x)$. By computer algebra (or manual computation),

$$\begin{aligned} W_{1,4}(1,2,x) &= 16384x^8 - 8192x^6 + 1280x^4 - 63x^2 \\ &= x^2 \cdot \big(16384x^6 - 8192x^4 + 1280x^2 - 63\big). \end{aligned}$$

Since $u \neq 0$, it is a root of the second factor above. By computer algebra, this polynomial of degree 6 is irreducible. Thus, Proposition 3.1(A) implies that u and, consequently, the cyclic pentagon are non-constructible. Therefore, $5 \in \mathrm{NCL}(2)$.

Next, let $n = 6$, let $0 < a, b \in \mathbb{R}$, $k \in \{1, 2, 3\}$, $m := 6 - k$, and consider the cyclic hexagon (4.1). (Note that the order of edges is irrelevant when we investigate the constructibility of cyclic n-gons.) If $a = b$, then the cyclic hexagon is regular and constructible. If $k = 1$, then computer algebra (or manual computation) says that

$$W_{1,5}(a, b, x) = x \cdot (-16b^5x^4 + 20b^3x^2 + a - 5b);$$

the second factor is quadratic in x^2. Since $u \neq 0$ is a root of the second factor of $W_{1,5}(a, b, x)$ by Lemma 4.2(iii), u^2, u, and the hexagon are constructible. Similarly,

$$\begin{aligned} W_{2,4}(a,b,x) &= 8b^4x^4 + (-8b^2 - 2a^2)x^2 + 2, \text{ and} \\ W_{3,3}(a,b,x) &= x \cdot \big((4b^3 - 4a^3)x^2 - 3b + 3a\big), \end{aligned}$$

and we conclude the constructibility for $k \in \{2, 3\}$ in the same way. Note that $W_{3,3}(a, b, x)$ is the zero polynomial if $a = b$; however, this case reduces to the constructibility of the regular hexagon. Therefore, the cyclic hexagon is constructible from its side lengths if there are at most two distinct side lengths.

To prove that $6 \in \mathrm{NCL}(3)$, we quote the method of Czédli and Szendrei [3, IX.2.7]; the only difference is that here we choose integer side lengths. Using the cosine angle addition identity, it is easy to conclude that, for all $\kappa_1, \kappa_2, \kappa_3 \in \mathbb{R}$ such that $\kappa_1 + \kappa_2 + \kappa_3 = \pi$,

$$(\cos\kappa_1)^2 + (\cos\kappa_2)^2 + (\cos\kappa_3)^2 + 2\cos\kappa_1 \cdot \cos\kappa_2 \cdot \cos\kappa_3 - 1 = 0\,. \tag{4.5}$$

The cyclic hexagon $P_6(a_1, \ldots, a_6) := P_6(1, 1, 2, 2, 3, 3)$ exists by (3.1). We will apply Proposition 3.1(A). Let $\alpha_1, \ldots, \alpha_6$ be the corresponding central half angles. Define $\kappa_1/2 = \alpha_1 = \alpha_2$, $\kappa_2/2 = \alpha_3 = \alpha_4$, $\kappa_3/2 = \alpha_5 = \alpha_6$, and $u = (1/2r)^2$, where r is the radius of the circumscribed circle. We have $\cos\kappa_1 = \cos(2\alpha_1) = 1 - 2\cdot(\sin\alpha_1)^2 = 1 - 2(a_1/2r)^2 = 1 - 2a_1^2 u = 1 - 2u$. We obtain $\cos\kappa_2 = 1 - 8u$ and $\cos\kappa_3 = 1 - 18u$ similarly. Since $\kappa_1+\kappa_2+\kappa_3 = \pi$, we can substitute these equalities into (4.5). Hence, we obtain that u is a root of the cubic polynomial $h_1(x) = 144x^3 - 196x^2 + 28x - 1$. Thus, $2u$ is a root of $h_2(x) = 18y^3 - 49y^2 + 14y - 1$. Computer algebra says that this polynomial is irreducible. Therefore, $P_6(1,1,2,2,3,3)$ is not constructible. This completes the proof of Theorem 1.1 (i) and (ii), because the Gauss–Wantzel theorem takes care of $7 \in \mathrm{NCL}(1)$. ∎

Parts from the proof of Proposition 1.3 ([3])**.** Let $n = 3$. With $d_1 = 1$, $d_2 = 2$ and $d_3 = 3$, (4.5) and the formulas analogous to (3.13) give that $12x^3+14x^2-1 = 0$. Substituting $x = y/2$, we obtain that $2u = 2/r$ is a root of $h_3(y) = 3y^3 + 7y^2 - 2$. Since none of $\pm1, \pm2, \pm1/3$ and $\pm2/3$ is a root of $h_3(y)$, this polynomial is irreducible. Hence, we conclude that the triangle $D_3(1,2,3)$ is not constructible.

Next, following Czédli and Szendrei [3, IX.1.27], we deal with the cyclic quadrangle $D_4(d_1,\dots,d_4)$, see Figure 1.1. Since $\alpha_1+\alpha_2+\alpha_3+\alpha_4 = \pi$, we have $\cos(\alpha_1+\alpha_2) = -\cos(\alpha_3+\alpha_4)$. Hence, using the cosine angle addition identity and rearranging and squaring twice, we obtain

$$\begin{aligned}\sum_{j=1}^{4}(\cos\alpha_j)^4 - 2\cdot\sum_{1\le j<s\le 4}(\cos\alpha_j)^2(\cos\alpha_s)^2 + \\ + 4\cdot\cos\alpha_1\cdot\cos\alpha_2\cdot\cos\alpha_3\cdot\cos\alpha_4\cdot\Bigl(-2+\sum_{j=1}^{4}(\cos\alpha_j)^2\Bigr) + \\ + 4\cdot\sum_{1\le j<s<t\le 4}(\cos\alpha_j)^2(\cos\alpha_s)^2(\cos\alpha_t)^2 = 0.\end{aligned} \tag{4.6}$$

Clearly, if we substitute $\cos\alpha_j$ in (4.6) by $d_j u$, for $j = 1,\dots,4$, and divide the equality by u^4, then we obtain that $u = 1/r$ is a root of a polynomial of the form $c_2x^2 + c_0$. A straightforward calculation (preferably, by computer algebra) shows that this polynomial is not the zero polynomial since

$$c_2 = 4(d_1d_2 + d_3d_4)(d_1d_3 + d_2d_4)(d_1d_4 + d_1d_3).$$

Thus $u = 1/r$ is constructible, and so is $D_4(d_1,\dots,d_4)$.

Next, let $n = 5$, and let $d_1 = d_2 = 499$, $d_3 = d_4 = 500$ and $d_5 = 501$; observe that $D_5(d_1,\dots,d_5)$ exists. With $u = 1/r$ as before, $\cos(2\alpha_1) = 2(\cos\alpha_1) - 1 = 2(d_1u)^2 - 1$, $\cos(2\alpha_3) = 2\cdot(d_3u)^2 - 1$, and $\cos\alpha_5 = d_5u$. Applying (4.5) to $\kappa_1 = 2\alpha_1$,

$\kappa_2 = 2\alpha_3$, and $\kappa_3 = \alpha_5$, we obtain with the help of computer algebra that u is a root of the polynomial

$$1\,494\,006\,000\,000x^5 + 498\,005\,992\,004x^4 - 5\,988\,012x^3 - 1\,995\,995x^2 + 6x + 1.$$

Since this polynomial is irreducible, $D_5(d_1, \ldots, d_5)$ is not constructible . Thus, 5 belongs to NCD(3). ∎

5. Comments on Schreiber's argument

Roughly speaking, "quadratic irrationalities" are generally understood as expressions built from their variables and given constants with the help of the four arithmetic operations $+, -, \cdot, /$, and $\sqrt{}$; these operations can be used only finitely many times. Note that Schreiber [25] does not contain the definition of this well-known concept. By *our convention*, to be formulated exactly later in Definition 6.1, the *domain* of such a function is the largest subset D of $\mathbb{R}$ such that for all $u \in D$, the expression makes sense in the natural way *without* using complex numbers and *without* taking limits. For example, the domain $\mathrm{Dom}(f)$ of the function

$$f = \sqrt{-1 - x^2} + x - \sqrt{-1 - x^2} \tag{5.1}$$

is empty, while the domain of the function $g(x) := R_6(a_1, \ldots, a_6, x)$ given by

$$R_6(a_1, \ldots, a_5, x) = \sqrt{a_1} + \cdots + \sqrt{a_5} + \sqrt{1/x} - \sqrt{1/(x + x^2)}. \tag{5.2}$$

is $\mathrm{Dom}(g) = (0, \infty)$.

The first problem with Schreiber's argument is that quadratic irrationalities are not everywhere continuous in general. It can happen that they are not even defined where [25] needs their continuity. Nothing excludes the possibility that, say, a_n is the denominator of a subterm (or several subterms). This is exemplified by $n = 6$ and R_6 above with a_6 in place of x; then $R_6(a_1, \ldots, a_{n-1}, 0)$ is not a meaningful expression, because $0 \notin \mathrm{Dom}(g)$. Compare this phenomenon with "for $a_n = 0$, the quadratic irrationality R describes" from Section 2. One could argue against us by saying that, as it is straightforward to see,

$$\lim_{t \to 0+0} R_6(a_1, \ldots, a_5, t) = \sqrt{a_1} + \cdots + \sqrt{a_5},$$

so we could extend the domain of g to contain 0, and then g would be continuous (from the right) at 0 and, what is more important, the limit is again a quadratic irrationality. However, there are much more complicated expressions than (5.2).

Even if R_6 is only an artificial example without concrete geometric meaning, is it always straightforward to see that the limit is again a quadratic irrationality? As opposed to [25], we think that this question has to be raised; for a possible answer, see the rest of the present paper.

One could also argue against our strictness at the domain of f from (5.1); so we note that while $\sqrt{}$ is a single-valued continuous function on $[0,\infty) \subseteq \mathbb{R}$, we know, say, from Gamelin [6, page 171] that

$$\sqrt{} \text{ cannot be a single-valued continuous operation on an open disk of complex numbers centered at 0, not even on a punctured disk.} \tag{5.3}$$

Hence, complex numbers could create additional problems without solving the problem raised on vanishing denominators like those in (5.2).

The second problem is of geometrical nature. Note, however, that this problem is not as important as the first one, because Schreiber does not refer to constructibility programs or similar concepts. Hence, our aim in this paragraph is only to indicate the geometric background of the difficulty. Assume that the cyclic n-gon is constructible in general. Take a constructibility program that witnesses this. A step (1.3) can threaten the problem that the ninth and the thirteenth points are distinct for all $a_n > 0$ but they coincide for $a_n = 0$, and then they do not determine a line. Then this step does not work for $a_n = 0$. Similarly, another step may require to take the intersection of two lines, but if these two lines coincide for $a_n = 0$, then they do not determine their intersection point. If so, then this step cannot be a part of a constructibility program. Therefore, a constructibility programs that works for some n may be useless with one of the side lengths being 0.

The problems above show that no matter if we use algebraic tools like R_6 or geometric tools like constructibility programs, the induction step from $n-1$ to n is not as simple as [25] seems to expect. On the other hand, Remark 9.4 later will show that the surprising last sentence of Proposition 1.3 does not contradict Schreiber's argument. However, even Proposition 1.3 makes it desirable to give a precise treatment to Schreiber's idea by determining its scope of applicability.

6. Basic facts on field extensions

In this section, the reader is assumed to be familiar with basic field theory. We will need $\sqrt{}$ as a *continuous* single-valued function. Hence, supported by (5.3), we prefer the field $\mathbb{R}$ of real numbers to the field $\mathbb{C}$ of complex numbers in the present paper. Let K be an abstract field, $c \in K$, and assume that c is distinct from the square of any element of K. Denoting by $\sqrt{c}$ a new symbol that is subject to the computational rule $(\sqrt{c})^2 = c$, it is well known that

$$K(\sqrt{c}\,) := \{a + b\sqrt{c} : a, b \in F\} \tag{6.1}$$

is a field, a *quadratic field extension* of K. We know that K is a subfield of $K(\sqrt{c}\,)$ under the natural embedding $a \mapsto a + 0 \cdot \sqrt{c}$. Furthermore, for every $u \in K(\sqrt{c}\,)$,

$$\text{there exists a unique } \langle a, b\rangle \in K \times K \text{ such that } u = a + b\sqrt{c}. \tag{6.2}$$

Here, $a + b\sqrt{c}$ is the so-called *canonical form* of u. If $c = d^2$ for some $d \in K$, then $K(\sqrt{c}\,)$ still makes sense but it is K and (6.2) fails. By the uniqueness theorem of simple algebraic field extensions, see, for example, Dummit and Foote [4, Theorem 13.8, page 519], we have the following uniqueness statement: if K and K' are fields, $\varphi\colon K \to K'$ is an isomorphism, $c \in K$ is not a square in K, and $c' = \varphi(c)$, then

$$\begin{gathered}\text{there exists a } \textit{unique} \text{ extension } \psi\colon K(\sqrt{c}\,) \to K'(\sqrt{c'}\,) \text{ of } \varphi \text{ such that}\\ \psi(\sqrt{c}\,) = c', \text{ and } \psi \text{ is defined by the rule } \psi(a + b\sqrt{c}\,) = \varphi(a) + \varphi(b)\sqrt{c'}.\end{gathered} \tag{6.3}$$

Now, for a subfield K of $\mathbb{R}$ and $u \in \mathbb{R}$, we say that u *is a real quadratic number over* K if there exist an $m \in \mathbb{N}_0$ and a tower

$$K = K_0 \subset K_1 \subset \cdots \subset K_m \tag{6.4}$$

of field extensions such that K_j is a quadratic extension of K_{j-1} for all $j \in \{1, \dots, m\}$ and $u \in K_m \subseteq \mathbb{R}$. Note that if $u \in \mathbb{R}$ is real quadratic over K, then it is also algebraic over K, but not conversely. Let us emphasize that the concept of real quadratic numbers does not rely on $\mathbb{C}$ at all. For example, the equation $a = \sqrt{-6} \cdot \sqrt{-2}$ is not allowed to show that a is a real quadratic number over $\mathbb{Q}$.

For a subfield M of $\mathbb{R}$, M is *closed with respect to real square roots* if $\sqrt{c} \in M$ for all $0 \le c \in M$. Now let K be a subfield of $\mathbb{R}$. Using two towers of quadratic field extensions, see (6.4), it is routine to check that if $u, v \in \mathbb{R}$ are real quadratic numbers over K, then so are $u + v$, $u - v$, uv and, if $v > 0$, u/v and $\sqrt{v}$. Therefore, with the notation $K^{\square} := \{u \in \mathbb{R} : u \text{ is a real quadratic number over } K\}$,

$$\begin{gathered}K^{\square} \text{ is the smallest subfield of } \mathbb{R} \text{ that includes } K\\ \text{and is closed with respect to real square roots.}\end{gathered} \tag{6.5}$$

We will call $K^{\square}$ the *real quadratic closure* of K.

Next, assume that $a_1, \dots, a_n \in \mathbb{R}$ define a real number $b = b(a_1, \dots, a_n)$ geometrically, which we want to construct. For example, the a_i can be the side lengths of a cyclic n-gon and b can denote the radius of the circumscribed circle of that n-gon. In the language of constructibility programs, see around (1.3), this means that we are given the points $\langle 0,0\rangle$, $\langle 1,0\rangle$, $\langle a_1,0\rangle$, …, $\langle a_n,0\rangle$ on the real line, and we want to construct $\langle b,0\rangle$. In this situation, to ease the terminology, we simply say that we want to *construct a number* $b\in\mathbb{R}$ from $a_1,\dots,a_n\in\mathbb{R}$. By a well-known basic theorem on geometric constructibility, see [3],

$$\begin{gathered} b \text{ is constructible from } a_1,\dots,a_n \text{ iff } b \text{ is a real quadratic} \\ \text{number over } \mathbb{Q}(a_1,\dots,a_n)\text{, that is, iff } b\in\mathbb{Q}(a_1,\dots,a_n)^{\square}. \end{gathered} \tag{6.6}$$

This statement is a more or less straightforward translation of constructibility programs from Section 1 to an algebraic language, because the existence of intermediate points described by the program guarantee that we do not have to abandon $\mathbb{R}$ while computing the coordinates; see [3]. Note that, using basic field theory, it is straightforward to deduce Proposition 3.1(C) from (6.6).

Next, we deal with the algebraic background of the situation where one of the parameters in a geometric construction is treated as a variable. For a subfield F of $\mathbb{R}$, let $F[x]$ denote the *polynomial ring* over F. It consists of *polynomials*, which are sequences of their coefficients. So a polynomial is just a formal string, not a function, and the same will hold for the elements of the $F_j\langle x\rangle$ in (6.8) below. However, with any element $f\in F_j\langle x\rangle$, we will associate a *function* ${}^{\star}\!f$ in a natural way. Note that F is a subfield of $F[x]$, because every element of F is a so-called constant polynomial. The *field of fractions* over $F[x]$ is denoted by $F(x)$. It consists of formal fractions f_1/f_2 where $f_1,f_2\in F[x]$ and f_2 is not the zero polynomial. We say that $f_1/f_2=g_1/g_2$ iff $f_1g_2=f_2g_1$. Note that F is a subfield of $F(x)$, because $F[x]$ is a subring of $F(x)$. The element $x\in F(x)$ is *transcendental over* F, and $F(x)$ is a simple transcendental field extension of F. If $c\in\mathbb{R}$ is a transcendental number over F, that is, c is not a root of any non-zero polynomial with coefficients in F, then $F(c)$ is the smallest subfield of $\mathbb{R}$ including $F\cup\{c\}$. As a counterpart of (6.3), the *uniqueness theorem of simple transcendental extensions* asserts that if F and F' are fields, $\varphi\colon F\to F'$ is an isomorphism, $F(c)$ and $F'(c')$ are field extensions such that c and c' are transcendental over F and F', respectively, then

$$\text{there exists a } \textit{unique} \text{ extension } \psi\colon F(c)\to F'(c') \text{ of } \varphi \text{ such that } \psi(c)=c'; \tag{6.7}$$

see Dummit and Foote [4, page 645]. Note that we use x or y for the transcendental element over F and call it an *indeterminate* if we are thinking of evaluating it, but we use $c,d,\dots$ for real numbers that are transcendental over $F\subseteq\mathbb{R}$. However, say, $F(y)$ and $F(c)$ in these cases are isomorphic by (6.7); field theory in itself does not make a distinction between indeterminates and transcendental elements. A terminological comment: just because we make a distinction between a polynomial f and the function ${}^{\star}\!f$, we call $F(x)$ the *field of polynomial fractions* over F (with indeterminate or variable x) but, as opposed to many references, we shall avoid to call it a *function field.* A *tower of quadratic field extensions over* $F(x)$ is a finite increasing chain

$$\begin{gathered}F(x) = F_0\langle x\rangle \subset F_1\langle x\rangle \subset \cdots \subset F_k\langle x\rangle, \text{ where } F_j\langle x\rangle = F_{j-1}\langle x\rangle(\sqrt{d_j}\,)\\ \text{and } d_j \in F_{j-1}\langle x\rangle \text{ is not a square in } F_{j-1}\langle x\rangle \text{ for } j \in \{1,\dots,k\}.\end{gathered} \tag{6.8}$$

Note that x in the notation $F_k\langle x\rangle$ reminds us that (6.8) starts from $F(x)$ rather than, say, from $F(y)$ or $\mathbb{Q}$. (We cannot write $F_j[x]$ and $F_j(x)$, because they would denote a polynomial ring of and a transcendent extension over an undefined field F_j.)

Definition 6.1. Given (6.8) and $f \in F_k\langle x\rangle$, we define a (real-valued) *function* ${}^\star\! f$ *associated with* f and its *domain* $\mathrm{Dom}({}^\star\! f)$ by induction as follows.

- (i) If $f \in F[x]$ is a polynomial over F, then ${}^\star\! f$ is the usual function this polynomial determines and $\mathrm{Dom}({}^\star\! f) = \mathbb{R}$.
- (ii) Assume that $f \in F_0\langle x\rangle = F(x)$. Then we write f in the form $f = f_1/f_2$ such that $f_1, f_2 \in F[x]$ are relatively prime polynomials; this is always possible and the roots of f_2 are uniquely determined. We let $\mathrm{Dom}(f) = \mathbb{R} \setminus \{\text{real roots of } f_2\}$, and let ${}^\star\! f$ be the function defined by the rule ${}^\star\! f(r) = {}^\star\! f_1(r)/{}^\star\! f_2(r)$ for $r \in \mathrm{Dom}({}^\star\! f)$.
- (iii) Assume $j \geq 1$ and that ${}^\star d_j$ and $\mathrm{Dom}({}^\star d_j)$ have already been defined. We let $\mathrm{Dom}({}^\star(\sqrt{d_j}\,)) = \{r \in \mathrm{Dom}({}^\star d_j) : {}^\star d_j(r) \geq 0\}$. For $r \in \mathrm{Dom}({}^\star(\sqrt{d_j}\,))$, let ${}^\star(\sqrt{d_j}\,)(r)$ be the unique non-negative real number whose square is ${}^\star d_j(r)$.
- (iv) Assume that $f \in F_j\langle x\rangle$. By (6.2), there are unique f_1, f_2 in $F_{j-1}\langle x\rangle$ such that $f = f_1 + f_2\sqrt{d_j}$. We let $\mathrm{Dom}({}^\star\! f) = \mathrm{Dom}({}^\star\! f_1) \cap \mathrm{Dom}({}^\star\! f_2) \cap \mathrm{Dom}({}^\star(\sqrt{d_j}\,))$ and, for $r \in \mathrm{Dom}({}^\star\! f)$, ${}^\star\! f(r) := {}^\star\! f_1(r) + {}^\star\! f_2(r) \cdot {}^\star(\sqrt{d_j}\,)(r)$.

Two functions are considered *equal* if they have the same domain and they take the same values on their common domain. Usually, $f_1 \neq f_2 \in F_k\langle x\rangle$ does not imply ${}^\star\! f_1 \neq {}^\star\! f_2$. For example, $\mathrm{Dom}({}^\star(\sqrt{-1-x^2})) = \emptyset = \mathrm{Dom}({}^\star(\sqrt{-1-x^4}))$ and ${}^\star(\sqrt{-1-x^2}) = {}^\star(\sqrt{-1-x^4})$, but $\sqrt{-1-x^2} \neq \sqrt{-1-x^4}$. This explains why we make a notational distinction between f and ${}^\star\! f$ in general. Note that for a polynomial $f \in F[x] \subseteq F(x) = F_0(x)$, especially for $f(x) = x^n$, this distinction is not necessary, and we are not always as careful as in this section. That is,

$$\begin{gathered}\text{We often write } f(c) \text{ for } c \in F \text{ rather than } {}^\star\! f(c), \text{ if } f \text{ is a polynomial}\\ \text{or, in later sections, if } f = f_1/f_2 \text{ where } f_1 \text{ and } f_2 \text{ are polynomials.}\end{gathered} \tag{6.9}$$

Due to the following lemma, which will often be applied without referring to it, the distinction between f and ${}^\star\! f$ will not cause difficulty.

Lemma 6.2. *Given (6.8) and $f, g \in F_k\langle x\rangle$, let $r \in \mathrm{Dom}({}^\star f) \cap \mathrm{Dom}({}^\star g)$. Then ${}^\star(f+g)(r) = {}^\star f(r) + {}^\star g(r)$ and ${}^\star(fg)(r) = {}^\star f(r) \cdot {}^\star g(r)$.*

Proof. For $k = 0$, the statement is trivial. The induction step for the product runs as follows. Assume that $f, g \in F_j\langle x\rangle$. To save space, let $z = {}^\star(\sqrt{d_j})(r)$. Using Definition 6.1, the induction hypothesis, and $z^2 = {}^\star d_j(r)$, we obtain that

$$\begin{aligned}
{}^\star(fg)(r) &= {}^\star\big((f_1 + f_2\sqrt{d_j}\,)(g_1 + g_2\sqrt{d_j}\,)\big)(r)\\
&= {}^\star\big(f_1g_1 + f_2g_2d_j + (f_1g_2 + f_2g_1)\sqrt{d_j}\,\big)(r)\\
&= {}^\star(f_1g_1 + f_2g_2d_j)(r) + {}^\star(f_1g_2 + f_2g_1)(r)\cdot z\\
&= {}^\star f_1(r)\,{}^\star g_1(r) + {}^\star f_2(r)\,{}^\star g_2(r)\,{}^\star d_j(r) + {}^\star f_1(r)\,{}^\star g_2(r)z + {}^\star f_2(r)\,{}^\star g_1(r)z\\
&= ({}^\star f_1(r) + {}^\star f_2(r)z)\cdot({}^\star g_1(r) + {}^\star g_2(r)z) = {}^\star f(r)\cdot{}^\star g(r).
\end{aligned}$$

The evident treatment for addition is omitted. ■

Lemma 6.3. *For a subfield $F \subseteq \mathbb{R}$ and $f \in F_k\langle x\rangle$, assume that ${}^\star f$ has infinitely many roots in $\mathrm{Dom}({}^\star f)$. Then $f = 0$ in $F_k\langle x\rangle$ and ${}^\star f\colon \mathbb{R} \to \{0\}$ with $\mathrm{Dom}({}^\star f) = \mathbb{R}$.*

Proof of Lemma 6.3. We use induction on k. First, assume that $k = 0$. Then $f = f_1/f_2 \in F(x)$ where $f_1, f_2 \in F[x]$ are relatively prime polynomials and f_2 is not the zero polynomial. Necessarily, f_1 is the zero polynomial (with no nonzero coefficient), because otherwise ${}^\star f_1$ and ${}^\star f$ would only have finitely many roots. Therefore, in the field $F(x)$, f_1 and $f = f_1/f_2$ are the zero element, as required.

Next, assume that $k > 0$ and the lemma holds for $k-1$. Using (6.1), (6.2), and the notation given in (6.8), we obtain that there are unique $f_1, f_2 \in F_{k-1}\langle x\rangle$ such that $f = f_1 + f_2\sqrt{d_k}$. We can assume that $f_2 \neq 0$, because otherwise $f \in F_{k-1}\langle x\rangle$ and the induction hypothesis applies. Let $\overline{f} = f_1 - f_2\sqrt{d_k} \in F_k\langle x\rangle$, and define $g := f \cdot \overline{f} = f_1^2 - f_2^2 d_k$. Since $\mathrm{Dom}({}^\star g) \supseteq \mathrm{Dom}({}^\star f) = \mathrm{Dom}({}^\star\overline{f})$, if $y \in \mathrm{Dom}({}^\star f)$ is a root of ${}^\star f$, then ${}^\star g(y) = {}^\star f(y)\,{}^\star\overline{f}(y) = 0 \cdot {}^\star\overline{f}(y) = 0$ shows that ${}^\star g(y) = 0$. Thus, ${}^\star g$ has infinitely many roots. On the other hand, $g \in F_{k-1}\langle x\rangle$, so the induction hypothesis gives that $g = 0$ in $F_{k-1}\langle x\rangle$. Therefore, $f_1^2 = f_2^2 d_k$ and d_k is the square of $f_1/f_2 \in F_{k-1}\langle x\rangle$, contradicting (6.8). ■

Corollary 6.4. *Using the notation of (6.8), assume that $g_1, g_2 \in F_k\langle x\rangle$ are such that $\mathrm{Dom}({}^\star g_1) \cap \mathrm{Dom}({}^\star g_2)$ is infinite. Then $g_1 = g_2$ if and only if ${}^\star g_1 = {}^\star g_2$.*

Proof. Apply Lemma 6.3 for $f := g_1 - g_2 \in F_k\langle x\rangle$. ■

7. Power series with dyadic exponents

In this section, the references aim at well-known facts from calculus and complex analysis; most readers do not need these outer sources. However, some minimum knowledge of calculus is assumed. Because of (5.3), we mainly study real numbers. A *strict right neighborhood of* 0 is an open interval $(0, \varepsilon)$ where $0 < \varepsilon \in \mathbb{R}$. The adjective "strict" is used to emphasize that a strict right neighborhood of 0 does not contain 0. Since $x^{2^{-k}}$ for $k \in \mathbb{N}$ is not defined if $x < 0$, we only consider strict right neighborhoods of 0. A *dyadic number* is a rational number of the form $a \cdot 2^t$ where $a, t \in \mathbb{Z}$. Subfields of $\mathbb{R}$ closed with respect to real square roots were defined right before (6.5). The goal of this section is to prove the following theorem.

Theorem 7.1. *Let F be a subfield of $\mathbb{R}$ such that F is closed with respect to real square roots. Also, let $k \in \mathbb{N}_0$, and consider a tower (6.8) of quadratic field extensions of length k over $F(x)$. Finally, let $f \in F_k\langle x\rangle$, and assume that there is a strict right neighborhood $(0, \varepsilon)$ of 0 such that $(0, \varepsilon) \subseteq \mathrm{Dom}({}^\star f)$. Then there exist an integer $t \in \mathbb{Z}$ and elements $b_t, b_{t+1}, b_{t+2}, \dots$ in the field F such that*

$$ {}^\star f(x) = \sum_{j=t}^{\infty} b_j \cdot x^{j \cdot 2^{-k}} \tag{7.1} $$

holds in some strict right neighborhood of 0. Furthermore, if $f \neq 0$, then $b_t \neq 0$ and $t, b_t, b_{t+1}, b_{t+2}, \dots$ are uniquely determined.

Let us emphasize that t in (7.1) can be negative. Before proving this theorem, we need a lemma; f below has nothing to do with $F_k\langle x\rangle$.

Lemma 7.2. *Assume that $0 < \varepsilon \in \mathbb{R}$, $f\colon (0, \varepsilon) \to \mathbb{R}$ is a non-negative function, and*

$$ f(x) = 1 + \sum_{j=1}^{\infty} a_j x^j \qquad (\textit{with real coefficients } a_j) \tag{7.2} $$

for all $x \in (0, \varepsilon)$. Let b_j denote the real numbers defined recursively by

$$ b_j = \begin{cases} a_j/2 - \sum_{t=1}^{\lfloor j/2 \rfloor} b_t b_{j-t}, & \textit{if } j \textit{ is odd,} \\ a_j/2 - b_{j/2}^2 - \sum_{t=1}^{j/2-1} b_t b_{j-t}, & \textit{if } j \textit{ is even,} \end{cases} \tag{7.3} $$

for $j \in \mathbb{N}$. Then, in an appropriate strict right neighborhood of 0,

$$ \sqrt{f(x)} = 1 + \sum_{j=1}^{\infty} b_j x^j . \tag{7.4} $$

By basic properties of the radius of convergence, see, e.g., Rudin [19, Subsection 10.5 in page 198], the series in (7.2) is also convergent in $(-\varepsilon, \varepsilon)$; however, the function $f(x)$ need not be defined for $x \in (-\varepsilon, 0]$.

Proof of Lemma 7.2. First, we show the existence of a power series that represents $\sqrt{f}$ in the sense of (7.4), but we do not require the validity of (7.3) at this stage. We know that, for $x \in (-1,1)$, the *binomial series*

$$\sum_{j=0}^{\infty} \binom{1/2}{j} x^j = 1 + \frac{\frac{1}{2}}{1!}x + \frac{\frac{1}{2}(\frac{1}{2}-1)}{2!}x^2 + \frac{\frac{1}{2}(\frac{1}{2}-1)(\frac{1}{2}-2)}{3!}x^3 + \cdots \tag{7.5}$$

is absolutely convergent and it converges to $\sqrt{1+x}$ on $(-1,1)$; see, for example, Wrede and Spiegel [28, page 275]. Therefore, the same series defines a holomorphic function $g(z)$ on the open disk $D_1 = \{z \in \mathbb{C} : |z| < 1\}$ of complex numbers. Note that, for $z \in D_1$, $g(z)$ is one of the complex values of $\sqrt{1+z}$. Since both the series (7.5) and the function $\sqrt{1+x}$ are continuous on $(-1,1)$ and they take the same *positive* value at $x = 0$, we obtain that $g(x) = \sqrt{1+x}$ for any real $x \in (-1,1)$. Observe that $\sum_{j=1}^{\infty} a_j x^j$ in (7.2) is convergent and differentiable on the open disk $D_\varepsilon = \{z \in \mathbb{C} : |z| < \varepsilon\}$. By its continuity, $|\sum_{j=1}^{\infty} a_j x^j| < 1$ on an appropriate small open disc D_δ, where $\delta < \varepsilon$. Furthermore, as any power series within its radius of convergence, $\sum_{j=1}^{\infty} a_j x^j$ is differentiable on D_δ. Therefore, the composite function $g(\sum_{j=1}^{\infty} a_j x^j)$ is also differentiable on D_δ. Hence, by a basic property of holomorphic functions, there exists a power series $1 + \sum_{j=1}^{\infty} b_j x^j$, without stipulating (7.3), such that $g(\sum_{j=1}^{\infty} a_j x^j) = \sum_{j=0}^{\infty} b_j x^j = 1 + \sum_{j=1}^{\infty} b_j x^j$ for all complex $x \in D_\delta$; see, for example, Rudin [19, Theorem 10.16 in page 207]. Here, $b_0 = 1$ follows from $g(0) = 1$. In particular, for all real x in a small strict right neighborhood of 0,

$$\sqrt{f(x)} = \sqrt{1 + \textstyle\sum_{j=1}^{\infty} a_j x^j} = g(\textstyle\sum_{j=1}^{\infty} a_j x^j) = 1 + \textstyle\sum_{j=1}^{\infty} b_j x^j.$$

This proves the existence of an appropriate power series such that (7.4) holds in a strict right neighborhood of 0, but we still have to show the validity of (7.3).

Since the power series in (7.4) is absolute convergent in a small strict right neighborhood of 0, its product with itself converges to $\big(\sqrt{f(x)}\,\big)^2 = f(x)$; see, for example, Wrede and Spiegel [28, Theorem 5 in Chapter 11, page 269]. Therefore,

$$\begin{aligned} f(x) = 1 &+ (b_1 + b_1)x + (b_2 + b_1 b_1 + b_2)x^2 + \\ &+ (b_3 + b_1 b_2 + b_2 b_1 + b_3)x^3 + \\ &+ (b_4 + b_1 b_3 + b_2 b_2 + b_3 b_1 + b_4)x^4 + \\ &+ (b_5 + b_1 b_4 + b_2 b_3 + b_3 b_2 + b_4 b_1 + b_5)x^5 + \\ &+ (b_6 + b_1 b_5 + b_2 b_4 + b_3 b_3 + b_4 b_2 + b_5 b_1 + b_6)x^6 + \cdots . \end{aligned} \tag{7.6}$$

The power series converging to a function is unique; see, for example, Rudin [19, Corollary to Theorem 10.6 in page 199]. Consequently, comparing the coefficients in (7.6) with those in (7.2), we obtain that (7.3) holds. ■

Proof of Theorem 7.1. First, to prove the uniqueness part, assume that (7.1) holds for all $x \in (0, \varepsilon)$. Substituting ξ^{2^k} for x, we obtain that, for all $\xi \in (0, \varepsilon^{2^{-k}})$, ${}^\star f(\xi^{2^k}) = \sum_{j=t}^{\infty} b_j \xi^j = \sum_{s=0}^{\infty} b_{s+t} \xi^{s+t}$. There are two ways to continue. First, we can consider the function $g(z) := {}^\star f(z^{2^k})$ of a complex variable z and then we can refer to the uniqueness of its Laurent series expansion; e.g., see Gamelin [6, page 168]. Second, and more elementarily, we can observe that $\xi^{-t} \cdot {}^\star f(\xi^{2^k}) = \sum_{j=0}^{\infty} b_{j+t} \cdot \xi^j$ for all $\xi \in (0, \varepsilon^{2^{-k}})$. However, the power series of a function is unique; see, e.g., Rudin [19, Corollary to Theorem 10.6 in page 199]. The uniqueness of the coefficients in $\sum_{j=0}^{\infty} b_{j+t} \cdot \xi^j$ implies the uniqueness part of the theorem.

We prove the existence part of the theorem by induction on k. If $k = 0$, then $f = f_1/f_2$ for some relatively prime polynomials $f_1, f_2 \in F[x]$. If ${}^\star f_2(0) \neq 0$, then there exists an open circular disc D of positive radius with center 0 such that ${}^\star f_2$ has no zeros in $D \subset \mathbb{C}$. Since ${}^\star f$ in $\mathrm{Dom}({}^\star f)$ equals ${}^\star f_1 / {}^\star f_2$ and both the numerator and the denominator are polynomial functions, ${}^\star f$ is holomorphic in D and its Taylor series, which is of form (7.1) with $t = k = 0$, converges to ${}^\star f(x)$ by a well-known property of holomorphic functions; see, e.g., Rudin [19, Theorem 10.16 in page 207]. Furthermore, since the coefficients of the Taylor series are obtained by repeated derivations, they belong to F. The other case, where ${}^\star f_2(0) = 0$, reduces to the above case easily as follows. Assume that ${}^\star f_2(0) = 0$. Then there are a unique $n \in \mathbb{N}$ and a unique $g \in F[x]$ such that $f_2(x) = x^n \cdot g(x)$ and ${}^\star g(0) \neq 0$. By the previous case, ${}^\star(f_1/g)$ is represented by its Taylor series with coefficients in F. We can multiply this series by x^{-n} componentwise, see for example, Gamelin [6, page 173]. In other words, we multiply the series with ${}^\star(x^{-n})$. In this way, we obtain the Laurent series of ${}^\star(f_1/g) \cdot x^{-n} = {}^\star((f_1/g) \cdot x^{-n}) = {}^\star f$ with the same coefficients but "shifted" to the left by n. Thus, we obtain a series (7.1) with $t = -n$ and $k = 0$, which converges to ${}^\star f$ in a strict right neighborhood of 0, as required.

Next, we assume that $k > 0$ and that the theorem holds for $k - 1$. Combining (6.1) and (6.8), we obtain that f is of the form $f = f_1 + f_2\sqrt{d_k}$ where $f_1, f_2, d_k \in F_{k-1}\langle x \rangle$. Since the validity of the existence part of the theorem is obviously inherited from the summands to their sum when we add two functions, it suffices to deal with $f_2\sqrt{d_k}$ in case f_2 in $F_{k-1}\langle x \rangle$ is distinct from 0. Note at this point that the validity of the existence part of the theorem for f_2 is also inherited if we change f_2 to $-f_2$. We know from Lemma 6.3 that ${}^\star f_2$ and ${}^\star d_k$ only have finitely many roots in their domains. Therefore, decreasing the strict right neighborhood of 0 if necessary, we can assume that ${}^\star(f_2{}^2 \cdot d_k)$ has no root in $(0,\varepsilon)$ at all. Since this function is composed from the four arithmetic operations and square roots, it is continuous on its domain. Hence, either ${}^\star f_2$ is positive on $(0,\varepsilon)$, or it is negative on $(0,\varepsilon)$. We can assume that ${}^\star f_2$ is positive on $(0,\varepsilon)$, because in the other case we could work with ${}^\star(-f_2) = -{}^\star f_2$ similarly. Also, ${}^\star d_k$ is nonnegative on $(0,\varepsilon)$, because $(0,\varepsilon) \subseteq \mathrm{Dom}({}^\star f)$. Hence ${}^\star(f_2\sqrt{d_k}\,)$ and ${}^\star(\sqrt{f_2{}^2 \cdot d_k})$ agree on the interval $(0,\varepsilon)$. Since we are only interested in our function on $(0,\varepsilon)$, it suffices to deal with ${}^\star(\sqrt{f_2{}^2 \cdot d_k})$ rather than ${}^\star(f_2\sqrt{d_k}\,)$. By the induction hypothesis, ${}^\star(f_2{}^2 d_k)$ can be given in form (7.1), with $k-1$ in place of k. To simplify the notation, we will write f rather than $f_2{}^2 d_k$. So, $f \in F_{k-1}\langle x\rangle$ and ${}^\star f$ is positive on a strict right neighborhood of 0. By the induction hypothesis, we have a unique series below with all the c_j in F and $c_t \neq 0$ such that

$$ {}^\star f(x) = \sum_{j=t}^{\infty} c_j \cdot x^{j\cdot 2^{1-k}} \tag{7.7} $$

in a strict right neighborhood of 0. Note that (7.7) may fail for $x = 0$. Taking out the first summand from (7.7) and writing s for $j-t$, we obtain that

$$ {}^\star f(x) = c_t \cdot x^{t\cdot 2^{1-k}} \cdot \sum_{s=0}^{\infty} \frac{c_{s+t}}{c_t} \cdot x^{s\cdot 2^{1-k}} = c_t \cdot x^{t\cdot 2^{1-k}} \cdot \Bigl(1 + \sum_{s=1}^{\infty} a_s y^s\Bigr), $$

where $a_s := c_{s+t}/c_t \in F$ and $y := x^{2^{1-k}} = x^{2\cdot 2^{-k}}$. The rightmost infinite sum above is convergent in a strict right neighborhood of 0, because so is (7.7). Applying Lemma 7.2 with $b_0 := 1$ and b_j defined by (7.3) and replacing $t+2j$ by s in the next step, we obtain

$$ \begin{aligned} {}^\star(\sqrt{f}\,)(x) = \sqrt{{}^\star f(x)} &= \sqrt{c_t} \cdot x^{t\cdot 2^{-k}} \cdot \sum_{j=0}^{\infty} b_j y^j = \sum_{j=0}^{\infty} b_j \sqrt{c_t} \cdot x^{(t+2j)\cdot 2^{-k}} \\ &= \sum_{s=t}^{\infty,\bullet} b_{(s-t)/2} \cdot \sqrt{c_t} \cdot x^{s\cdot 2^{-k}} = \sum_{s=t}^{\infty} d_s \cdot x^{s\cdot 2^{-k}} \end{aligned} \tag{7.8} $$

in some right neighborhood of 0, where $\bullet$ means that only those subscripts s occur for which $s \equiv t \pmod 2$, and we have that $d_s := b_{(s-t)/2} \cdot \sqrt{c_t}$ for $s \equiv t \pmod 2$, and $d_s := 0$ otherwise. Since the a_s are all in F, the b_j given by (7.3) are also in F. Since ${}^\star f$ is positive in a (small) strict right neighborhood of 0 and, as x tends to 0, the series in (7.7) is dominated by $c_t \cdot x^{t\cdot 2^{1-k}}$, we obtain in a straightforward way that $c_t > 0$. Hence, $\sqrt{c_t} \in F$, because F is closed with respect to real square roots, and we conclude that $d_j \in F$ for $j \in \{t, t+1, t+2 \dots\}$. This completes the inductive step and the proof of Theorem 7.1. ∎

8. Puiseux series and historical comments

Now, we are going to compare Theorem 7.1 to known results; the rest of the paper does not rely on this section. Let F be a subfield of the field $\mathbb{C}$ of complex numbers. A *Puiseux series* over F is a generalized power series of the form

$$\sum_{j=t}^{\infty} b_j \cdot x^{j/m}, \tag{8.1}$$

where $m \in \mathbb{N}$, $t \in \mathbb{Z}$, and $b_j \in F$ for $j \in \{t, t+1, t+2, \dots\}$. In other words, a Puiseux series is obtained from a Laurent series with finitely many powers of negative exponent by substituting $\sqrt[m]{x}$ for its variable. Note that, for $w \in \mathbb{C} \setminus \{0\}$, the substitution $\sum_{j=t}^{\infty} b_j \cdot w^{j/m}$ of w for x in (8.1) is understood so that first we fix one of the m values of $\sqrt[m]{w}$, and then we use *this* value of $\sqrt[m]{w}$ to define $w^{j/m}$ as $\left(\sqrt[m]{w}\right)^j$, for all $t \le j \in \mathbb{Z}$. This convention allows us to say that certain Puiseux series are convergent in a punctured disk $D_\varepsilon^+ = \{z \in \mathbb{C} : 0 < |z| < \varepsilon\}$. This concept and the following theorem go back to Isaac Newton [17, 23].

Theorem 8.1. (Puiseux's Theorem, [21, 22]; see also [18, 20, 23]) *Let $F \subseteq \mathbb{C}$ be a field, and let*

$$P(x, y) = A_0(x) + A_1(x)y + \dots + A_n(x)y^n \tag{8.2}$$

be an irreducible polynomial in $F[x, y] = F[x][y]$ such that the $A_j[x]$ belong to $F[x]$ and $A_n(x) \neq 0$. If F is algebraically closed, then there exist a (small) positive $\varepsilon \in \mathbb{R}$ and a Puiseux series (8.1) such that this series converges to a function $Y(x)$ in the punctured disk D_ε^+ and, for all $x \in D_\varepsilon^+$, we have that $P(x, Y(x)) = 0$.

Note that $Y(x)$ above is a multiple-valued function in general and it is rarely continuous in D_ε^+. This is exemplified by $P(x, y) = y^2 - x \in \mathbb{C}[x][y]$ together with (5.3), where the Puiseux series is the one-element sum $x^{1/2}$. Note also that Theorem 8.1 seems not to imply Theorem 7.1 in a straightforward way, because $F_k\langle x \rangle$ is not an algebraically closed field for a finitely generated field F. Actually, Theorem 8.1 only implies a weaker form of Theorem 7.1. This weaker form asserts that the b_j belong to the algebraic closure of $F(x)$; this statement is useless at geometric constructibility problems. Fortunately, as our proof witnesses, it was possible to tailor Puiseux's proof to the peculiarities of Theorem 7.1.

9. A limit theorem for geometric constructibility

The aim of this section is to prove the following statement. For the constructibility of numbers, see (6.6).

Theorem 9.1. (Limit Theorem for Geometric Constructibility) *Let $a_1, \ldots, a_m$, and d be real numbers such that d is geometrically constructible from $a_1, \ldots, a_m$. Let $u(x)$ be a real-valued function. If there exist a positive $\varepsilon \in \mathbb{R}$ and a nonzero polynomial W of two indeterminates over $\mathbb{R}$ such that*

(i) *$u(x)$ is defined on the interval $(d, d+\varepsilon)$,*

(ii) *every coefficient in W is geometrically constructible from $a_1, \ldots, a_m$, and $W(c, u(c)) = 0$ holds for all $c \in (d, d+\varepsilon)$ such that c is transcendental over $\mathbb{Q}(a_1, \ldots, a_m)$,*

(iii) *for all $c \in (d, d+\varepsilon)$ such that c is transcendental over $\mathbb{Q}(a_1, \ldots, a_m)$, $u(c)$ is geometrically constructible from $c, a_1, \ldots, a_m$, and*

(iv) *$\lim_{x\to d+0} u(x) \in \mathbb{R}$ exists,*

then $\lim_{x\to d+0} u(x)$ is geometrically constructible from $a_1, \ldots, a_m$.

Clearly, if we require the equality and the constructibility in (ii) and (iii), respectively, for all elements c of the interval $(d, d+\varepsilon)$, not only for the transcendental ones, then we obtain a corollary with simpler assumptions. However, we shall soon see that Theorem 9.1 is more useful than its corollary just mentioned.

Remark 9.2. To show that (ii) in Theorem 9.1 is essential, we have the following example. As usual, $\lfloor\ \rfloor$ will stand for the (lower) integer part function. Let $\varepsilon = 1$, $d = 0$, and $m = 0$. For $x \in (0, 1)$, let $j(x) = -\lfloor \log_{10}(x) \rfloor \in \mathbb{Z}$. We define $u(x)$ by $u(x) := \lfloor 10^{j(x)} \cdot \pi \rfloor \cdot 10^{-j(x)}$, where $\pi = 3.141\,592\,653\,589\,793\ldots$, as usual. For example, if $x = 0.000\,000\,201\,502\,13$, then $j(x) = 7$ and $u(x) = 3.141\,592\,6 \in \mathbb{Q}$. Clearly, $\lim_{x\to 0+0} u(x) = \pi \in \mathbb{R}$ and, for every $c \in (0, 1)$, $u(c) \in \mathbb{Q}$ is constructible. Note that $u(c)$ is the root of the rational polynomial $x - u(c)$ with constructible coefficients, but this polynomial depends on c. All assumptions of Theorem 9.1 hold except (ii). If the theorem held without assuming (ii), then π would be geometrically constructible over $\mathbb{Q}$, which would contradict (6.6) by Lindemann [15]. Alternatively, it would be a contradiction because Squaring the Circle is impossible. Therefore, (ii) cannot be omitted from Theorem 9.1.

Remark 9.3. Consider the function $u\colon (0, 1) \to \mathbb{Q}$ from the previous remark. For each $c \in (0, 1)$, $u(c)$ is constructible from 0, 1, and c. However, based on Theorem 9.1, it is not hard to prove that $u(x)$ is not constructible from 0, 1, and x in the sense of (1.4); the details of this proof are omitted. This example points out that the meaning of "in general not constructible" needs a definition; an appropriate definition will be given in Remark 10.2.

Remark 9.4. The assumption that d is geometrically constructible from $a_1, \ldots, a_m$ cannot be omitted from Theorem 9.1.

Proof of Remark 9.4. Our argument is based on Proposition 1.3. Suppose, for a contradiction, that Theorem 9.1 without assuming that d is constructible, referred to as the *forged theorem*, holds. Let d_1, d_2, d_3 be arbitrary positive real numbers such that $D_3(d_1, d_2, d_3)$ exists. Note that $\langle 3, d_1, d_2, d_3\rangle$ will play the role of $\langle m, a_1, \ldots, a_m\rangle$ in the forged theorem. Denote by $r(d_1, d_2, d_3)$ the radius of the circumscribed circle of $D_3(d_1, d_2, d_3)$, and let $d := -r(d_1, d_2, d_3)$. By geometric reasons, there is a positive $\varepsilon \in \mathbb{R}$ such that $D_4(d_1, d_2, d_3, -x)$ exists for all $x \in (d, d+\varepsilon)$; just think of an infinitesimally small fourth side. Let $u(x)$ denote the radius of the circumscribed circle of $D_4(d_1, d_2, d_3, -x)$. We know from Proposition 1.3 that $D_4(d_1, d_2, d_3, -c)$ is constructible from d_1, d_2, d_3, c, provided $c \in (d, d+\varepsilon)$. Hence, $u(c)$ is also constructible and (iii) of the forged theorem holds. It is straightforward to conclude from (4.4) that so does (ii), while the satisfaction of (i) is evident. Since the geometric dependence of $u(x)$ on x is continuous, $\lim_{x\to d+0} u(x) = r(d_1, d_2, d_3) \in \mathbb{R}$. So, (iv) is also satisfied. Hence, by the forged theorem, $r(d_1, d_2, d_3) = \lim_{x\to d+0} u(x)$ is geometrically constructible from d_1, d_2, d_3. Therefore, $D_3(d_1, d_2, d_3)$ is also constructible from d_1, d_2, d_3. However, this contradicts Proposition 1.3, completing the proof of Remark 9.4. ■

We will derive Theorem 9.1 from the following, more technical, statement.

Proposition 9.5. *Let F be a subfield of $\mathbb{R}$ such that F is closed with respect to real square roots, and let $d \in F$. Assume that $W \in F[x, y] \setminus \{0\}$ is a nonzero polynomial. If $\langle c_j : j \in \mathbb{N}\rangle$ and $\langle u_j : j \in \mathbb{N}\rangle$ are sequences of real numbers such that*

(i) *c_j is transcendental over F and $d < c_j$, for all $j \in \mathbb{N}$,*
(ii) *for all $j \in \mathbb{N}$, u_j is a real quadratic number over $F(c_j)$, see (6.4),*
(iii) *$W(c_j, u_j) = 0$, for all $j \in \mathbb{N}$, and*
(iv) *$\lim_{j\to\infty} c_j = d$ and $\lim_{j\to\infty} u_j \in \mathbb{R}$,*

then $\lim_{j\to\infty} u_j \in F$.

As a preparation to the proof of Proposition 9.5, we need two lemmas. In the first of them, all sorts of intervals, for example, $[a, b)$, (a, ∞), $(-\infty, b]$, (a, b), etc., are allowed, and the empty union is the empty set.

Lemma 9.6. *If F is a subfield of $\mathbb{R}$, $k \in \mathbb{N}$, $F_k\langle x\rangle$ is as in (6.8), and $f \in F_k\langle x\rangle$, then $\mathrm{Dom}({}^{\star}f)$ is the union of finitely many intervals and ${}^{\star}f$ is continuous on each of these intervals.*

Proof. We use induction on k. If $f \in F_0(x) = F(x)$, then $f = f_1/f_2$ where $f_1, f_2 \in F[x]$ are polynomials. Hence, ${}^{\star}f_2$ only has finitely many (real) roots and the statement for $k = 0$ is clear. Next, assume that $k > 0$ and that the lemma holds for $k-1$. Lemma 6.3 gives that ${}^\star d_k$ has only finitely many roots. By the induction hypothesis, $\mathrm{Dom}({}^\star d_k)$ is the union of finitely many intervals and ${}^\star d_k$ is continuous on each of these intervals. Thus, it follows from continuity that $\mathrm{Dom}({}^\star(\sqrt{d_k}\,))$ is the union of finitely many intervals; see Definition 6.1(iii). Furthermore, by the continuity of $\sqrt{}$ on $[0,\infty)$, ${}^\star(\sqrt{d_k}\,)$ is continuous on these intervals. Now, addition and multiplication preserves continuity. Furthermore, the intersection of two (and, consequently, three) sets that are unions of finitely many intervals is again the union of finitely many intervals. Therefore, see Definition 6.1(iv), the lemma holds for $f = f_1 + f_2 \cdot \sqrt{d_k} \in F_k\langle x\rangle$. ∎

The *restriction* of a map φ to a set A is denoted by $\varphi\rceil_A$. The *identity map* $A \to A$, defined by $a \mapsto a$ for all $a \in A$, is denoted by id_A. Next, we prove a technical lemma.

Lemma 9.7. *Let F be a subfield of $\mathbb{R}$, and let $c \in \mathbb{R}$ be a transcendental element over F. Assume that*

$$F(c) = K_0 \subset K_1 \subset \cdots \subset K_k \tag{9.1}$$

is a tower of quadratic field extensions such that $K_k \subseteq \mathbb{R}$. Then there exists a tower (6.8) of quadratic field extensions over $F(x)$ of length k and there are field isomorphisms $\varphi_j\colon F_j\langle x\rangle \to K_j$ for $j \in \{0,\dots k\}$ such that

(i) *$\varphi_0\rceil_F = \mathrm{id}_F$, $\varphi_0(x) = c$, and for all $j \in \{1,\dots k\}$, $\varphi_j\rceil_{F_{j-1}\langle x\rangle} = \varphi_{j-1}$;*

(ii) *for all $j \in \{0,\dots k\}$ and $f \in F_j\langle x\rangle$, we have $c \in \mathrm{Dom}({}^\star f)$ and $\varphi_j(f) = {}^\star f(c)$.*

Proof. We prove the lemma by induction on k. By (6.7), id_F extends to an isomorphism $\varphi_0\colon F(x) \to F(c)$ such that $\varphi_0(x) = c$ and $\varphi_0\rceil_F = \mathrm{id}_F$. Thus, for every $g = \sum a_i x^i \in F[x]$, we have that $\varphi_0(g) = \sum \varphi_0(a_i)\varphi_0(x)^i = \sum a_i c^i = {}^\star g(c)$. Since c is transcendental over F, ${}^\star f_2(c) \neq 0$ holds for all $f_2 \in F[x] \setminus \{0\}$. Hence, we obtain from Definition 6.1(i)–(ii) that $c \in \mathrm{Dom}({}^\star f)$ and $\varphi_0(f) = {}^\star f(c)$ hold for all $f \in F(x) = F_0(x)$. This settles the base, $k = 0$, of the induction.

Next, assume that $k > 0$ and the lemma holds for $k-1$. By (6.1) and $K_k \subseteq \mathbb{R}$, there exists a positive real number $e_k \in K_{k-1}$ such that $K_k = K_{k-1}(\sqrt{e_k})$ and e_k is not a square in K_{k-1}. Let $d_k = \varphi_{k-1}^{-1}(e_k)$. Since $\varphi_{k-1}\colon F_{k-1}\langle x\rangle \to K_{k-1}$ is an isomorphism, d_k is not a square in $F_{k-1}\langle x\rangle$. Furthermore, by the induction hypothesis,

$$c \in \mathrm{Dom}({}^\star d_k) \quad \text{and} \quad 0 < e_k = \varphi_{k-1}(d_k) = {}^\star d_k(c). \tag{9.2}$$

Define $F_k\langle x\rangle$ with the help of this d_k. That is, $F_k\langle x\rangle := F_{k-1}\langle x\rangle(\sqrt{d_k}\,)$. It follows from (6.2) that each element $f \in F_k\langle x\rangle$ can be written uniquely in the canonical form $f = f_1 + f_2 \cdot \sqrt{d_k}$, where $f_1, f_2 \in F_{k-1}\langle x\rangle$. By (6.3), φ_{k-1} extends to a (unique) isomorphism $\varphi_k\colon F_k\langle x\rangle \to K_k$, and φ_k is defined by the rule

$$\varphi_k(f_1 + f_2 \cdot \sqrt{d_k}) = \varphi_{k-1}(f_1) + \varphi_{k-1}(f_2) \cdot \sqrt{e_k}. \tag{9.3}$$

Clearly, Part (i) of the lemma holds. By the induction hypothesis, c belongs to $\mathrm{Dom}({}^\star f_1) \cap \mathrm{Dom}({}^\star f_2)$. Combining this containment with (9.2) and Definition 6.1(iv), we obtain that $c \in \mathrm{Dom}({}^\star f)$, for all $f = f_1 + f_2 \cdot \sqrt{d_k} \in F_k\langle x\rangle$, written in canonical form. Hence, using (9.3), Definition 6.1(iii)–(iv),

$$\begin{aligned}\varphi_k(f) &= \varphi_{k-1}(f_1) + \varphi_{k-1}(f_2) \cdot \sqrt{e_k} = {}^\star f_1(c) + {}^\star f_2(c) \cdot \sqrt{{}^\star d_k(c)} \\ &= {}^\star f_1(c) + {}^\star f_2(c) \cdot {}^\star(\sqrt{d_k})(c) = {}^\star f(c),\end{aligned}$$

as required. This completes the induction step and the proof of Lemma 9.7. ∎

Proof of Proposition 9.5. First, we only deal with the case $d = 0$. We can assume that $\lim_{j\to\infty} u_j \neq 0$, since otherwise $\lim_{j\to\infty} u_j \in F$ needs no proof. Consequently, for all but finitely many $j \in \mathbb{N}$, $u_j \neq 0$. After omitting finitely many initial members from our sequences, we can assume that,

$$\text{for all } j \in \mathbb{N},\ u_j \neq 0. \tag{9.4}$$

Let $F(x)^{\mathrm{acl}}$ denote the *algebraic closure* of the field $F(x)$. Note that no matter how we choose the d_j's in (6.8), $F_k\langle x\rangle \subseteq F(x)^{\mathrm{acl}}$. Consider one of our transcendental numbers, c_j, where $j \in \mathbb{N}$. Since u_j is a real quadratic number over $F(c_j)$, there exists a tower (9.1), with c_j in place of c, of quadratic field extensions such that $u_j \in K_k$. This tower and even its length k may depend on j. By Lemma 9.7, we obtain a tower of quadratic field extensions (6.8) together with an isomorphism $\varphi_k^{(j)}\colon F_k\langle x\rangle \to K_k$ and an $f_j \in F_k\langle x\rangle$, both depending on j, such that

$$\varphi_k^{(j)}\rceil_F = \mathrm{id}_F,\ \varphi_k^{(j)}(x) = c_j,\ c_j \in \mathrm{Dom}({}^\star f_j), \text{ and } u_j = \varphi_k^{(j)}(f_j) = {}^\star f_j(c_j). \tag{9.5}$$

We can write W in the unique form $W(x,y) = \sum_{\langle i,t\rangle\in B} a_{it}x^iy^t$, where B is a finite non-empty subset of $\mathbb{N}_0 \times \mathbb{N}_0$ and $a_{it} \in F$ for all $\langle i,t\rangle \in B$. We define $b_t := \sum_{\{i:\langle i,t\rangle\in B\}} a_{it}x^i \in F[x] \subseteq F(x) \subseteq F_k\langle x\rangle$ and $g = \sum_{t\in\mathbb{N}_0} b_ty^t \in F_k\langle x\rangle[y]$. This sum is finite and $g(f_j) \in F_k\langle x\rangle$. Actually, g corresponds to W under the canonical $F[x,y] \to F_k\langle x\rangle[y]$ embedding. Note that g does not depend on j. (Note also that we cannot write ${}^\star g$ here since ${}^\star g$ stands for a real-valued function.) Observe that $g \neq 0$ in $F_k\langle x\rangle[y]$, because $W \neq 0$. Using (9.5), we obtain that

$$\begin{aligned}\varphi_k^{(j)}\big(g(f_j)\big) &= \varphi_k^{(j)}\big(\sum_{t\in\mathbb{N}_0} b_t f_j^t\big) = \varphi_k^{(j)}\Big(\sum_{t\in\mathbb{N}_0}\big(\sum_{\{i:\langle i,t\rangle\in B\}} a_{it}x^i\big) f_j^t\Big)\\ &= \varphi_k^{(j)}\big(\sum_{\langle i,t\rangle\in B} a_{it}x^i f_j^t\big) = \sum_{\langle i,t\rangle\in B}\varphi_k^{(j)}(a_{it})\,\big(\varphi_k^{(j)}(x)\big)^i\,\varphi_k^{(j)}(f_j)^t\\ &= \sum_{\langle i,t\rangle\in B} a_{it}\,c_j^i\,u_j^t = W(c_j,u_j) = 0.\end{aligned}$$

This implies that $g(f_j) = 0$. Observe that $f_j \in F_k\langle x\rangle \subseteq F(x)^{\mathrm{acl}}$ and that $g \in F_k\langle x\rangle[y] \subseteq F(x)^{\mathrm{acl}}[y]$. Since g, as a polynomial over $F(x)^{\mathrm{acl}}$, has only finitely many roots in $F(x)^{\mathrm{acl}}$, $\{f_j : j \in \mathbb{N}\}$ is a finite subset of $F(x)^{\mathrm{acl}}$. Therefore, after thinning the sequence $\langle c_j : j \in \mathbb{N}\rangle$ if necessary, we can assume that f_j does not depend on j. Thus, we can let $f := f_j \in F_k\langle x\rangle$. This allows us to assume that, from now on, $F_k\langle x\rangle$ and the tower (6.8) do not depend on j. We obtain from (9.5) that

$$c_j \in \mathrm{Dom}({}^\star\! f) \text{ and } u_j = {}^\star\! f(c_j), \text{ for all } j \in \mathbb{N}. \tag{9.6}$$

We obtain from (9.4) and (9.6) that $f \neq 0$ in $F_k\langle x\rangle$. Combining Lemma 9.6 with (9.6), $0 = d < c_j$, and $\lim_{j\to\infty} c_j = 0$, we conclude that $(0,\varepsilon) \subseteq \mathrm{Dom}({}^\star\! f)$ for some positive $\varepsilon \in \mathbb{R}$. Therefore, Theorem 7.1 applies and

$${}^\star\! f(x) = \sum_{\ell=t}^{\infty} b_\ell \cdot x^{\ell\cdot 2^{-k}} =: \Sigma_1(x) \quad \text{in some strict right neighborhood of 0,} \tag{9.7}$$

where $b_t \neq 0$, $b_t, b_{t+1}, b_{t+2}, \ldots \in F$, and $t, b_t, b_{t+1}, b_{t+2}, \ldots$ are uniquely determined. We claim that t in (9.7) is non-negative. Suppose the contrary. Then the function

$$f_1(z) := \sum_{\ell=t}^{\infty} b_\ell \cdot z^\ell \tag{9.8}$$

has a pole at 0. It is straightforward to see and we also know from Spiegel et al. [24, page 175] that $\lim_{z\to 0}|f_1(z)| = \infty$. Therefore, since $\lim_{j\to\infty} c_j^{2^{-k}} = 0$ and since (9.7) gives ${}^\star\! f(x) = f_1(x^{2^{-k}})$ in some strict right neighborhood of 0, we obtain that

$$\lim_{j\to\infty}|u_j| = \lim_{j\to\infty}|{}^\star\! f(c_j)| = \lim_{j\to\infty}|f_1(c_j^{2^{-k}})| = \infty.$$

This contradicts the assumption $\lim_{j\to 0} u_j \in \mathbb{R}$. Thus, t in (9.7) is non-negative. Next, consider the power series $\Sigma_2(y) := \sum_{\ell=0}^{\infty} b_\ell \cdot y^\ell$ where, for $\ell < t$, we let $b_\ell := 0$. Since $\Sigma_2(y) = \Sigma_1(y^{2^k})$, $\Sigma_2(y)$ converges in some strict right neighborhood of 0.

Therefore, the radius of convergence of $\Sigma_2(y)$ is positive and $\Sigma_2(y)$ is continuous at 0; see, for example, Wrede and Spiegel [28, page 272]. Hence, using (9.6), (9.7), (9.8), and $\lim_{j\to\infty} c_j^{2^{-k}} = 0$,

$$\lim_{j\to\infty} u_j = \lim_{j\to\infty} {}^{\star}f(c_j) = \lim_{j\to\infty} \Sigma_1(c_j) = \lim_{j\to\infty} \Sigma_2(c_j^{2^{-k}}) = \Sigma_2(0) = b_0 \in F.$$

This proves Proposition 9.5 in the particular case $d = 0$.

Finally, if $d \in F$ is not necessarily 0, then we let $d' := 0$, $c_j' := c_j - d$, $u_j' := u_j$, and $W'(x,y) := W(x+d,y)$. It is straightforward to see that the primed objects satisfy the conditions of Proposition 9.5. Hence, applying the particular case, we conclude that $\lim_{j\to\infty} u_j = \lim_{j\to\infty} u_j' \in F$. ∎

Proof of Theorem 9.1. With the assumptions of the theorem, let F be the real quadratic closure of the field $\mathbb{Q}(a_1,\dots,a_m)$. Since d and the coefficients in W are constructible from $a_1,\dots,a_m$, (6.6) implies that d and these coefficients belong to F. So, W is polynomial over F of two indeterminates. Since F is a countable field, so is its algebraic closure, F^{acl}. Thus, the set of transcendental numbers over F is everywhere dense in $\mathbb{R}$. Hence, we can pick a sequence $\langle c_j : j \in \mathbb{N}\rangle$ of transcendental numbers over F such that $c_j \in (d, d+\varepsilon)$ for all $j \in \mathbb{N}$ and $\lim_{j\to\infty} c_j = d$. Define u_j by $u_j := u(c_j)$; it is constructible from $c_j, a_1,\dots,a_m$ by the assumptions. Using (6.6), we obtain that $u_j \in \mathbb{Q}(a_1,\dots,a_m,c_j)^{\square} = \big(\mathbb{Q}(a_1,\dots,a_n)^{\square}(c_j)\big)^{\square} = F(c_j)^{\square}$. That is, u_j is a real quadratic number over $F(c_j)$, for all $j \in \mathbb{N}$. We have $W(c_j,u_j) = W(c_j,u(c_j)) = 0$. Condition (iv) of Theorem 9.1 yields that $\lim_{j\to\infty} u_j = \lim_{j\to\infty} u(c_j)$ exists and equals $\lim_{x\to d+0} u(x) \in \mathbb{R}$. Now that all of its conditions are fulfilled, we can apply Proposition 9.5. In this way, we obtain that $\lim_{x\to d+0} u(x) = \lim_{j\to\infty} u_j \in F$. Therefore, (6.6) yields that $\lim_{x\to d+0} u(x)$ is constructible from $a_1,\dots,a_m$. This completes the proof of Theorem 9.1. ∎

10. The Limit Theorem at work

The aim of this section is to prove the following lemma.

Lemma 10.1. *If $n \ge 8$, then there exists a* transcendental *number $0 < c \in \mathbb{R}$ such that the cyclic n-gon*

$$P_n(c) = P_n(\underbrace{1,\dots,1}_{\ell\text{ copies}}, \underbrace{c,\dots,c}_{n-\ell\text{ copies}}), \text{ where } \ell = \begin{cases} 7, & \text{if } n \ne 14,\\ 9, & \text{if } n = 14,\end{cases} \tag{10.1}$$

exists but it is not constructible from 1 and c.

Proof of Lemma 10.1. Let $n \geq 8$. It follows from (3.1) that $P_n(b)$, defined as the polygon in (10.1) with b instead of c, exists for every real number $b \in (0,1)$. Suppose, for a contradiction, that $P_n(c)$ is constructible for all transcendental numbers $c \in (0,1)$. Define a function $u\colon (0,1) \to \mathbb{R}$ by $u(x) = 1/(2r_n(x))$, where $r_n(x)$ denotes the radius of the circumscribed circle of $P_n(x)$; see (10.1). We are going to use the Limit Theorem 9.1. Condition (i) of Theorem 9.1, denoted by 9.1(i), clearly holds with $\langle 0,1,2,0,1\rangle$ playing the role of $\langle d, \varepsilon, m, a_1, \dots, a_m\rangle$. Since $P_n(c)$ is constructible from 0, 1, and c for all $c \in (0,1)$, so is $u(c)$. Thus, 9.1(iii) is satisfied. The polynomial $W_{\ell,n-\ell}(1,x,y) \in \mathbb{Z}[x,y]\setminus\{0\}$ from Lemma 4.2(iii) shows that 9.1(ii) also holds. Since the geometric dependence of $r_n(x)$ on x is continuous, $r_n(x)$ tends to the radius r_ℓ of the regular ℓ-gon with side length 1 as $x \to 0+0$. Hence, $\lim_{x\to 0+0} u(x) = 1/(2r_\ell) \in \mathbb{R}$, and 9.1(iv) holds. Thus, we obtain from Theorem 9.1 that $1/(2r_\ell)$ is constructible from 0 and 1. Therefore, so is the regular ℓ-gon, which contradicts the Gauss–Wantzel theorem; see [27]. ∎

Remark 10.2. The proof of Lemma 10.1 above shows how one can complete Schreiber's original argument. As it is pointed out in Remark 9.3, first we need a definition. Rather than the opposite of (1.4), "in general not constructible" in (1.2) should be understood as "there are concrete side lengths such that the cyclic n-gon exists but not constructible". Second, one would need a generalization of Lemma 4.2(iii) for the case where the side lengths can be pairwise distinct. In this way, one could use Theorem 9.1 to prove (1.2). Since we are proving a stronger statement, Theorem 1.1, we do not elaborate these details.

Remark 10.3. The constructibility of the regular pentagon was already known by the classical Greek mathematics. Now, combining Theorem 9.1 with Theorem 1.1(b) and Lemma 4.2(iii), we obtain an unusual and quite complicated way to prove this well-known fact, because the radius of $P(1,1,1,1,1)$ is the limit of the radius of $P(1,1,1,1,1,y)$ as $y \to 0+0$.

11. Turning transcendental to rational

The aim of this section is to prove the following theorem.

Theorem 11.1. (Rational Parameter Theorem for geometric constructibility) *Let $I \subseteq \mathbb{R}$ be a nonempty open interval, let $a_1, \dots, a_m$ be arbitrary real numbers, and let $u\colon I \to \mathbb{R}$ be a continuous function. Denote $\mathbb{Q}(a_1,\dots,a_m)$ by K, and assume that there exists a polynomial $W \in K[x,y] \setminus \{0\}$ such that $W(x,u(x)) = 0$ holds for all $x \in I$. If there exists a number $c \in I$ such that c is transcendental over K*

and $u(c)$ is geometrically non-constructible from $a_1, \ldots, a_m$ and c, then there also exists a rational *number $c' \in I$ such that $u(c')$ is non-constructible from $a_1, \ldots, a_m$ and c'.*

In many cases, the continuity of u follows from geometric reasons. Our proof needs that u is continuous. Since the continuity of u does not follow if we define it implicitly by the polynomial equation $W(x, u(x)) = 0$, we stipulate it separately in the theorem above. Although Hilbert's irreducibility theorem, see later, is closely connected with Galois groups, we need the following lemma; this lemma will allow us to *simultaneously* deal with the irreducibility of a polynomial and the order of the corresponding splitting field extension, which is the same as the order of the corresponding Galois group. The following lemma is an easy reformulation of Proposition 3.1(C).

Lemma 11.2. *For a subfield L of $\mathbb{R}$, let $g(x) = b_k x^k + b_{k-1}x^{k-1} + \cdots + b_0 \in L[x]$ be an* irreducible *polynomial of degree $k \in \mathbb{N}$. Then the following two assertions hold.*

(i) *There are polynomials $g_0 \in L[y_1, \ldots, y_k]$, $g_1, \ldots, g_k \in L[y]$, $h_1 \in L[y,x]$, $h_2 \in L[y]$, and an* irreducible *polynomial $h \in L[y]$ such that*

$$g(x) - b_k \cdot \big(x - g_1(y)\big) \cdots \big(x - g_k(y)\big) = h(y)h_1(y,x) \quad \textit{holds in} \quad L[y,x] \tag{11.1}$$

$$\textit{and} \quad g_0\big(g_1(y), \ldots, g_k(y)\big) - y = h(y)h_2(y) \quad \textit{holds in} \quad L[y]. \tag{11.2}$$

(ii) *No matter how $h, h_1, h_2, g_0, g_1, \ldots, g_k$ are chosen in part (i), a root of g is constructible over L if and only if all roots of g are constructible over L if and only if the degree of h is a power of 2.*

Note that h and the other polynomials in (11.1) and (11.2) are not uniquely determined in general.

Proof of Lemma 11.2. First, we prove part (i). Let F denote the splitting field of g over L. Then there are $\alpha_1, \ldots, \alpha_k \in F$, the roots of g, such that

$$g(x) = b_k \cdot (x - \alpha_1) \cdots (x - \alpha_k) \text{ in } F[x] \text{ and } F = L(\alpha_1, \ldots, \alpha_k). \tag{11.3}$$

Since the degree $[F : L]$ of the field extension is finite and L is of characteristic 0, F is a simple algebraic extension of L; see, for example, Dummit and Foote [4, Theorem 14.25 in page 595]. Thus, there exists a $\beta \in F$ such that $F = L(\beta)$. Let $h \in L[y]$ be the minimal polynomial of β. Clearly, $h(y)$ is an irreducible polynomial. Using (11.3) and $F = L(\beta)$, we obtain polynomials g_i over L such that $\beta = g_0(\alpha_1, \ldots, \alpha_k)$ and $\alpha_j = g_j(\beta)$ for $j \in \{1, \ldots, k\}$. By the definition of these polynomials and (11.3),

$$g_0(g_1(\beta), \ldots, g_k(\beta)) - \beta = 0 \text{ in } F \text{ and} \tag{11.4}$$

$$g(x) - b_k \cdot (x - g_1(\beta)) \cdots (x - g_k(\beta)) = 0 \text{ in } F[x]. \tag{11.5}$$

We know that $F = L(\beta) \cong L[y]/(h(y))$ in the usual way, where β corresponds to $y + \big(h(y)\big)$; see, for example, Dummit and Foote [4, pages 512–513]. Hence, there is a unique surjective ring homomorphism $\varphi\colon L[y] \to F$, defined by the rule $\varphi(w(y)) \mapsto w(\beta)$. The kernel of this homomorphism is

$$\mathrm{Ker}(\varphi) = \big(h(y)\big), \text{ where the principal ideal is understood in } L[y]. \tag{11.6}$$

Note that the restriction $\varphi\rceil_L$ of φ to L is the identity map id_L. We can extend $\varphi \cup \{\langle x, x\rangle\}$ to a unique surjective ring homomorphism $\psi\colon L[y,x] = L[y][x] \to F[x]$. We claim that

$$\mathrm{Ker}(\psi) = \big(h(y)\big), \text{ understood in } L[y,x]. \tag{11.7}$$

To verify this, let $w(y,x) = \sum_{i=0}^{s} w_i(y)x^i \in L[y,x]$ and compute:

$$\begin{aligned} \psi\big(w(y,x)\big) = \psi\Big(\sum_{i=0}^{s} w_i(y)x^i\Big) &= \sum_{i=0}^{s} \varphi\big(w_i(y)\big)x^i = 0 \text{ in } F[x] \\ &\iff (\forall i)\, \varphi\big(w_i(y)\big) = 0 \overset{(11.6)}{\iff} (\forall i)\, h(y) \mid w_i(y) \text{ in } L[y] \\ &\iff h(y) \mid w(y,x) \text{ in } L[y,x], \text{ as required.} \end{aligned}$$

Using that $\psi\rceil_L = \varphi\rceil_L = \mathrm{id}_L$, we obtain that $\psi\big(g(x)\big) = g(x)$. Since ψ is a ring homomorphism and $\psi\big(x - g_i(y)\big) = \psi(x) - \psi\big(g_i(y)\big) = x - \varphi\big(g_i(y)\big) = x - g_i(\beta)$,

$$\begin{aligned} &\psi\big(g(x) - b_k \cdot (x - g_1(y)) \cdots (x - g_k(y))\big) \\ &\qquad = g(x) - b_k \cdot (x - g_1(\beta)) \cdots (x - g_k(\beta)) \overset{(11.5)}{=} 0. \end{aligned}$$

Combining this with (11.7), we obtain a polynomial $h_1(y,x) \in L[y,x]$ such that (11.1) holds. Similarly, the definition of φ gives that

$$\varphi\big(g_0(g_1(y), \dots, g_k(y)) - y\big) = g_0(g_1(\beta), \dots, g_k(\beta)) - \beta \overset{(11.4)}{=} 0.$$

Hence, (11.6) yields a polynomial $h_2 \in L[y]$ such that (11.2) holds. This proves part (i) of Lemma 11.2.

Second, in order to prove part (ii), assume that we have polynomials satisfying the conditions in part (i), including (11.1) and (11.2). Since h is irreducible, $F := L[y]/\big(h(y)\big)$ is a field. Let $\beta := y + \big(h(y)\big)$, which generates $L[y]/\big(h(y)\big)$, and let $\alpha_i = g_i(\beta) = g_i(y) + \big(h(y)\big) \in L[y]/\big(h(y)\big)$, for $i \in \{1, \dots, k\}$. Since $h(\beta) = 0$ and $h(y)$ is irreducible, it follows that h is the minimal polynomial of β. Substituting β for y and using that $h(\beta) = 0$, (11.1) shows that $g(x) = b_k \cdot (x - \alpha_1) \cdots (x - \alpha_k)$ in $F[x]$. Hence, F includes the splitting field $L(\alpha_1, \dots, \alpha_k)$ of g over L. On the other hand, the same substitution into (11.2) shows that $\beta = g_0(\alpha_1, \ldots, \alpha_k)$ belongs to the splitting field. Hence, $F = L(\beta) = L(\alpha_1, \ldots, \alpha_k)$ is (isomorphic to) the splitting field of g. It is well known that $[F : L] = [L(\beta) : L] = \deg h$; see, for example, Dummit and Foote [4, Theorem 13.4 in page 513]. Thus, part (ii) follows from Proposition 3.1(C).

■

Next, we recall Hilbert's irreducibility theorem, [11], from Fried and Jarden [5, page 219 and Proposition 13.4.1 in page 242], or [5, Theorem 13.3.5 in page 241] in a particular form we need it later; see also [10] for a short introduction.

Proposition 11.3. (Hilbert's irreducibility theorem) *Let $K \subseteq \mathbb{R}$ be a field, and let $T = \langle T_1, \ldots, T_s\rangle$ and $Y = \langle Y_1, \ldots, Y_k\rangle$ be two systems of variables. Let $f_1(T, Y)$, $\ldots$, $f_m(T, Y)$ be irreducible polynomials in Y with coefficients in the field $K(T)$. That is, $f_1, \ldots, f_m$ are irreducible in $K(T)[Y]$. Then there exists a system $a = \langle a_1, \ldots, a_s\rangle \in \mathbb{Z}^s$ of integers such that $f_i(a, Y)$ is defined and it is irreducible in $K[Y]$ for all $i \in \{1, \ldots, m\}$.*

The tuple $a = \langle a_1, \ldots, a_s\rangle$ above is called a common *specialization* of the polynomials $f_i(T, Y)$. The transition from $f_i(T, Y)$ to $f_i(a, Y)$ is called a *substitution*, or the $T := a$ *substitution*. The statement above says that finitely many irreducible polynomials have a common integer specialization. This easily implies that

$$\text{The } f_i(T, Y) \text{ above have infinitely many common integer specializations.} \tag{11.8}$$

To see this, suppose, for a contradiction, that there are only are finitely many common integer specializations $a^{(1)}, \ldots, a^{(\kappa)} \in \mathbb{Z}^s$. For $j \in \{1, \ldots, \kappa\}$, we define

$$f^{(j)} := \begin{cases} Y_1^2 - a_1^{(j)} T_1, & \text{if } \ a_1^{(j)} \neq 0, \\ Y_1^2 - T_1, & \text{if } \ a_1^{(j)} = 0. \end{cases}$$

Clearly, $f^{(j)}(T, Y)$ is irreducible in $K(T)[Y]$ but $f^{(j)}(a^{(j)}, Y)$ is reducible in $K[y]$. Therefore, applying Proposition 11.3 to the polynomials $f_1, \ldots, f_m, f^{(1)}, \ldots, f^{(\kappa)}$, we obtain a new common integer specialization of $f_1, \ldots, f_m$. This is a contradiction, which proves (11.8).

We will also need the following trivial fact, which says that, even if they are not defined everywhere, substitutions are partially defined ring homomorphism:

For $f(T, Y), g(T, Y) \in K(T)[Y]$ and a specialization $a \in \mathbb{Z}^s$, if the $T := a$ substitution is defined for $f(T, Y)$ and $g(T, Y)$, then it is also defined for and commutes with their sum and product. (11.9)

Proof of Theorem 11.1. Since $K[x,y] = K[x][y] \subseteq K(x)[y]$, we have that $W \in K(x)[y]$. We can assume that W is an irreducible polynomial in $K(x)[y]$. Suppose that this is not the case. Then there are a finite index set J, pairwise non-associated irreducible polynomials $W_j \in K(x)[y]$, and $\alpha_j \in \mathbb{N}$ such that $W(x,y) = \prod_{j\in J} W_j(x,y)^{\alpha_j}$. Using the isomorphism $K(x) \cong K(c)$, see (6.7), we obtain that the $W_j(c,y) \in K(c)[y]$ are also irreducible. From $W(c,u(c)) = 0$, we obtain that $u(c)$ is a root of some $W_j(c,y)$. Since non-associated irreducible polynomials cannot have a common root, there is exactly one $j \in J$ such that $W_j(c,u(c)) = 0$. Let $M := \min\bigl\{|W_i(c,u(c))| : i \in J \setminus \{j\}\bigr\}$. By the uniqueness of j, $M > 0$. The roots of the $W_i(c,y)$ depend continuously on the parameter c, and u is a continuous function. Hence, there is a small neighborhood of c such that for all c' in this neighborhood and for all $i \in J \setminus \{j\}$, we have that $|W_i(c',u(c'))| > M/2$. However, $0 = W(c',u(c')) = \prod_{i\in J} W_i(c',u(c'))^{\alpha_i}$ for all $c' \in I$. Thus, $W_j(c',u(c')) = 0$ for all c' in a small neighborhood of c. Therefore, after replacing I by this small neighborhood, W can be replaced by W_j in our considerations; this justifies the assumption that W is irreducible in $K(x)[y]$. Also, $W(c,y)$ is irreducible in $K(c)[y]$. Actually, we can assume even more. If we multiply (or divide) it by an appropriate polynomial from $K[x]$ if necessary, $W(x,y)$ becomes an irreducible polynomial in $K[x][y]$ by Gauss' Lemma; see Dummit and Foote [4, Proposition 9.5 and Corollary 9.6 in pages 303–304]. So, we assume $W(x,y)$ is *irreducible* in $K[x][y] = K[x,y]$ and also in $K(x)[y]$. We write $W(x,y)$ in the form

$$W(x,y) = a_k(x)y^k + a_{k-1}(x)y^{k-1} + \cdots + a_0(x), \text{ where } a_k,\dots,a_0 \in K[x], \tag{11.10}$$

$a_k(x) \neq 0$ and, since W is irreducible in $K[x][y]$, $a_0(x) \neq 0$. Note that $a_k(c) \neq 0$ and $a_0(c) \neq 0$, since c is transcendental over K. After shrinking the interval I if necessary, we can assume that

$$\text{for all } r \in I,\ a_k(r) \neq 0 \text{ and } a_0(r) \neq 0. \tag{11.11}$$

We are looking for an appropriate rational number c' within I, that is, near c. However, (11.8) can only give some very large $c' \in \mathbb{Z}$, which need not belong to I. To remedy this problem, we are going to translate the constructibility problem of $u(x)$ to an equivalent problem that is easier to deal with. To do so, we can assume that the open interval I is determined by two rational numbers, because otherwise we can take a smaller interval that still contains c. Let q be the middle point of I; it is a rational number, and I is of the form $I = (q-\delta, q+\delta)$, where $0 < \delta \in \mathbb{Q}$. We can assume that $q = 0$, because otherwise we can work with

$$\langle u^*(x) := u(x+q),\ W^*(x,y) := W(x+q,y),\ c^* := c-q\rangle$$

instead of $\langle u(x), W(x,y), c\rangle$; to justify this, observe that c^* is still transcendental over K. Note also that, by the uniqueness of simple transcendental field extensions, see (6.7), $\mathrm{id}_K \cup \{\langle x, x+q\rangle\}$ extends first to an automorphism of $K(x)$, and then to an automorphism of $K(x)[y]$ that maps W to W^*, and we conclude that W^* is irreducible over $K(x)$. We can also assume that W^* is irreducible over $K[x]$, because otherwise we can divide it by the greatest common divisor of its coefficients, which belongs to $K[x]\setminus\{0\}$, and Gauss' Lemma applies. Finally, for every $x \in \mathbb{R}$, $x+q$ is constructible from x and vice versa; so they are equivalent data modulo geometric constructibility.

So, from now on, $I = (-\delta, \delta)$. The punctured interval $I \setminus \{0\} = (-\delta, 0) \cup (0, \delta)$ will be denoted by I°. We also consider another open set,

$$J := \{r \in \mathbb{R} : |r| > 1/\delta\} = (-\infty, -1/\delta) \cup (1/\delta, \infty).$$

The functions $\tau\colon I^\circ \to J$, defined by $\tau(x) := 1/x$, and $\xi : J \to I^\circ$, defined by $\xi(t) := 1/t$, are reciprocal bijections and both are continuous on their domains. To emphasize that ξ and τ have disjoint domains, we often write $\xi(t)$ and $\tau(x)$ instead of $1/t$ and $1/x$, respectively. The compound function, $v\colon J \to \mathbb{R}$, defined by $v(t) = u(\xi(t))$ is also continuous. Since $\tau(x)$ is constructible from x and $\xi(t)$ is constructible from t, we obtain that

$$\begin{gathered}\text{The constructibility of } u(x) \text{ from } x \in I^\circ \text{ over } K \text{ is equivalent}\\ \text{to the constructibility of } v(t) = u(\xi(t)) \text{ from } t \in J \text{ over } K.\end{gathered} \tag{11.12}$$

Of course, "from $x \in I^\circ$ over K" is equivalent to "from $x \in I^\circ$ and $a_1, \dots, a_m$", and a similar comment applies for analogous situations. Using that both ξ and τ map rational numbers to rational numbers, we conclude from (11.12) that

$$\begin{gathered}\text{It suffices to find a } d' \in J \cap \mathbb{Q} \text{ such that}\\ v(d') \text{ is not constructible from } a_1, \dots, a_m.\end{gathered} \tag{11.13}$$

Let $d = \tau(c) = 1/c$; it is also transcendental over K. We obtain from (11.12) that $v(d)$ is not constructible from d over K. For $i \in \{0, \dots, k\}$, we define $\widetilde{b}_i(t) := a_i(\xi(t)) = a_i(1/t) \in K(t)$. Clearly, for a sufficiently large $j \in \mathbb{N}$, we obtain that $t^j \cdot \widetilde{b}_0(t), \dots, t^j \cdot \widetilde{b}_k(t) \in K[t]$, and we can take out the greatest common divisor from these polynomials. Hence, there is a polynomial $q(t) \in K[t]$ such that $\widehat{b}_0(t) := q(t)\widetilde{b}_0(t) \in K[t], \dots, \widehat{b}_k(t) := q(t)\widetilde{b}_k(t) \in K[t]$, and the greatest common divisor of $\widehat{b}_0(t), \dots, \widehat{b}_k(t)$ is 1. Observe that $1/t \in K(t)$ is a transcendental element over K and $K(t) = K(1/t)$. Thus, by the uniqueness of simple transcendental field extensions, see (6.7), $\mathrm{id}_K \cup \{\langle x, 1/t\rangle\}$ extends to an isomorphism of $K(x) \to K(t)$, and also to an isomorphism $K(x)[y] \to K(t)[y]$ such that $y \mapsto y$. This isomorphism maps

$a_i(x)$ to $a_i(1/t) = \widetilde{b}_i(t)$. Using this isomorphism and the fact that (11.10) is an irreducible polynomial over $K(x)$, we obtain that $\widetilde{b}_k(t)y^k + \cdots + \widetilde{b}_0(t) \in K(t)[y]$ is irreducible over $K(t)$. Multiplying this polynomial by $q(t)$, we obtain that

$$\widehat{W}(t,y) := \widehat{b}_k(t)y^k + \widehat{b}_{k-1}(t)y^{k-1} + \cdots + \widehat{b}_0(t) \in K[t][y] \tag{11.14}$$

is a polynomial that is irreducible in y over $K[t]$ and also over $K(t)$. For $t \in J$, let us compute:

$$\begin{aligned} \widehat{W}(t,v(t)) &= \widehat{b}_k(t) \cdot v(t)^k + \widehat{b}_{k-1}(t) \cdot v(t)^{k-1} + \cdots + \widehat{b}_0(t) \\ &= q(t)\big(a_k(\xi(t)) \cdot u(\xi(t))^k + \cdots + a_0(\xi(t))\big) \\ &= q(t) \cdot W\big(\xi(t), u(\xi(t))\big) = 0, \end{aligned} \tag{11.15}$$

because $\xi(t) \in I^\circ$. Therefore, $v(t)$, whose constructibility from t over K is investigated, is the root of the irreducible polynomial $\widehat{W}(t,y) \in K[t][y]$ in the sense that $\widehat{W}(t,v(t)) = 0$ for all $t \in J$, and we know that $v(d)$ is not constructible from the transcendental number $d \in J$ over K.

Let $L = K(d)$. Based on (11.14), we let

$$g^{(d)}(y) = \widehat{b}_k(d)y^k + \widehat{b}_{k-1}(d)y^{k-1} + \cdots + \widehat{b}_0(d) \in L[y].$$

Note that $g^{(d)}(y)$ is obtained from $\widehat{W}(t,y)$ by the $t := d$ substitution. Here, it is reasonable to denote the indeterminate of $g^{(d)}$, and that of $g^{(t)}$ to be defined soon, by y. However, when referring to (11.1), (11.2), or Lemma 11.2, then we change y to x without further warning. Since the polynomial in (11.14) is irreducible in y over $K(t)$ and $L = K(d) \cong K(t)$, we conclude that $g^{(d)}$ is irreducible in $L[y]$. Since d is transcendental over K, we can substitute d for t in (11.15). Note that $\widehat{W}$ is composed from polynomials and $\xi(t) = 1/t$, so

$$\text{any substitution for } t \text{ in (11.15) makes sense except for } t := 0. \tag{11.16}$$

In this way, we obtain that $v(d)$ is a root of $g^{(d)}$. By Lemma 11.2, there is an irreducible polynomial $h^{(d)}(y) \in L[y]$ and there are further polynomials $g_0^{(d)} \in L[y_1,\dots,y_k]$, $g_1^{(d)},\dots,g_k^{(d)},h_2^{(d)} \in L[y]$, and $h_1^{(d)} \in L[y,x]$ such that (11.1) and (11.2), with the superscript (d) added, hold. Since $v(d)$ is not constructible over L, Lemma 11.2 yields that $\deg_y(h^{(d)})$ is not a power of 2.

Observe that $\mathrm{id}_K \cup \{\langle d,t\rangle\}$ extends to a unique field isomorphism $\varphi_0\colon L = K(d) \to K(t)$, which extends further to a unique ring isomorphism $\varphi\colon L[y] \to K(t)[y]$ that maps y to y. Let $\widehat{h}(t,y)$ denote the φ-image of $h^{(d)}(y)$; we will also denote it by $h^{(t)}(y)$. (Note that $h^{(d)}(y)$ is obtained from $\widehat{h}(t,y)$ by the $t := d$

substitution; however d as a specialization is not so important, because we are only interested in *integer* specializations.) Clearly, $\deg_y(h^{(t)}) = \deg_y(h^{(d)})$, because d is transcendental over K. Using that φ preserves irreducibility, we obtain that $g^{(t)}(y)$ and $h^{(t)}(y)$ are irreducible polynomials in $K(t)[y]$, since so are $g^{(d)}(y)$ and $h^{(d)}(y)$ in $L[y]$. We define $g^{(t)}, g_1^{(t)}, \dots, g_k^{(t)}, h_2^{(t)} \in K(t)[y]$ as the φ-images of $g^{(d)}, g_1^{(d)}, \dots, g_k^{(d)}, h_2^{(d)} \in L[y]$, respectively. Note at this point that $g^{(t)}(y) = \widehat{W}(t,y)$; see (11.14). Hence, (11.15) and (11.16) give that

$$\text{For every } d' \in J,\ v(d') \text{ is a root of } g^{(d')}(y) := \widehat{W}(d',y). \tag{11.17}$$

We also define $g_0^{(t)} \in K(t)[y_1, \dots, y_k]$ as the image of $g_0^{(d)}$ under the unique extension of $\varphi_0 \cup \{\langle y_1, y_1\rangle, \dots, \langle y_k, y_k\rangle\}$ to a (unique) isomorphism $L[y_1, \dots, y_k] \to K(t)[y_1, \dots, y_k]$. We define $h_1^{(t)} \in K(t)[y,x]$ analogously. In this way, we have defined a "(t)-superscripted variant" over $K(t)$ of the system of polynomials occurring in Lemma 11.2. Since isomorphisms preserve (11.1) and (11.2), we conclude that

$$\begin{array}{l}\text{The } (t)\text{-superscripted family of our poly-}\\ \text{nomials satisfy (11.1) and (11.2).}\end{array} \tag{11.18}$$

Next, we apply Proposition 11.3 with $s = 1$ for the irreducible polynomials $g^{(t)}(y) = \widehat{W}(t,y)$ and $h^{(t)}(y) = \widehat{h}(t,y)$. In this way, taking (11.8) into account, we conclude that there are infinitely many specializations $d' \in \mathbb{Z}$ such that

$$\begin{array}{l} h^{(d')}(y) := \widehat{h}(d',y) \text{ and } g^{(d')}(y) = \widehat{W}(d',y) \text{ are}\\ \text{defined and they are irreducible in } K[y].\end{array} \tag{11.19}$$

We also specialize the polynomials $g_0^{(t)}, g_1^{(t)}, \dots, g_k^{(t)}, h_1^{(t)}, h_2^{(t)}$ by $t := d'$. Not every d' satisfying (11.19) is appropriate for this purpose, because the coefficients of these polynomials are fractions over $K[t]$ and some denominators may turn to zero if we substitute d' for t. Fortunately, there are only finitely many denominators with finitely many roots, so we still have infinitely many $d' \in Z$ that specialize all these additional polynomials such that (11.19) still holds. There are only finitely many of these d' such that the leading coefficient of $h^{(t)}$ diminishes at the specializations $t := d'$, and there are also finitely many d' outside J. Thus, there exists a $d' \in J \cap \mathbb{Z}$ such that (11.19) holds, all the "(t)-superscripted" polynomials can be specialized by $t := d'$, and $\deg_y(h^{(d')}) = \deg_y(h^{(t)}) = \deg_y(h^{(d)})$, which is not a power of 2. Combining (11.9) and (11.18), we obtain that the (d')-superscripted family of polynomials satisfy (11.1) and (11.2). Therefore, by Lemma 11.2(ii), no root of $g^{(d')}(y) \in K[y]$ is constructible over K. But $v(d')$ is a root of $g^{(d')}(y)$ by (11.17), whence $v(d')$ is not constructible over K. That is, $v(d')$ is not constructible from $a_1, \dots, a_m$ that generate the field K. Thus, (11.13) completes the proof of Theorem 11.1. ■

12. Completing the proof of Theorem 1.1

We only have to combine some earlier statements.

Proof of Theorem 1.1. Parts (i) and (ii) are proved in Section 4. Part (iii) is proved in Section 3 in an elementary way. For $n \geq 8$, Lemma 10.1 proves that there exist an appropriate $\ell \in \{7,9\}$ and a positive transcendental number $c \in \mathbb{R}$ such that $P_n(c) = P(1,\dots,1,c,\dots,c)$ given in (10.1) exists but it is not constructible from its sides. In other words, $P_n(c)$ is geometrically not constructible from 0, 1 and c. We conclude from (3.1) that there exists a small open interval I such that $c \in I$ and $P_n(x) = P(1,\dots,1,x,\dots,x)$ exists for all $x \in I$. Let $r_n(x)$ denote the radius of the circumscribed circle of $P_n(x)$. Now, we are in the position to apply Theorem 11.1 with $m = 2$, $a_1 = 0$, $a_2 = 1$, $u(x) = 1/(2r_n(x))$, and $W(x,y) := W_{\ell,n-\ell}(1,x,y)$; see Lemma 4.2(iii). In this way, we can change c to an appropriate rational number $c' \in I$ such that $P_n(c') = P(1,\dots,1,c',\dots,c')$ still exists but it is not constructible from its sides, 1 and c'. We can write c' in the form c'_1/c'_2 where $c'_1, c'_2 \in \mathbb{N}$. Clearly, $P(c'_2,\dots,c'_2,c'_1,\dots,c'_1)$ is non-constructible, because it is geometrically similar to $P_n(c')$. Therefore, $n \in \mathrm{NCL}(2)$. This proves parts (iii) and (iv) of Theorem 1.1. ∎

References

[1] P. M. Cohn, *Algebra. I. 2nd edition*, J. Wiley and Sons, 1982.

[2] D. A. Cox, Why Eisenstein proved the Eisenstein criterion and why Schönemann discovered it first, *The American Mathematical Monthly*, **118** (2011), 3–21.

[3] G. Czédli and Á. Szendrei, *Geometric constructibility*, Polygon, Szeged, 1997 (in Hungarian).

[4] DS. Dummit and R. M. Foote, *Abstract Algebra*, John Wiley and Sons, 2004.

[5] M. D. Fried and M. Jarden, *Field Arithmetic. 3rd ed.*, revised by Moshe Jarden, Springer, 2008.

[6] T. W. Gamelin, *Complex Analysis*, Springer, 2001.

[7] W. J. Gilbert and W. K. Nicholson, *Modern Algebra with Applications. 2nd ed.*, J. Wiley and Sons, 2004.

[8] G. Grätzer, *Universal Algebra. 2nd edition*, Springer, 2008.

[9] I. N. Herstein, *Abstract Algebra. 3rd ed.*, John Wiley and Sons, 1999.

[10] http://en.wikipedia.org/wiki/Hilbert's_irreducibility_theorem

[11] D. Hilbert, Über die Irreduzibilität ganzer rationaler Funktionen mit ganzzahligen Koeffizienten, *Journal für die reine und angewandte Mathematik*, **110** (1892), 104–129.

[12] N. Jacobson, *Basic Algebra I*, W. H. Freeman and Co., San Francisco, 1974.

[13] I. Kersten, *Algebra*, Universitätsverlag Göttingen, 2006.

[14] E. W. Kiss, *Introduction to Abstract Algebra*, Typotex, Budapest, 2007 (in Hungarian).

[15] F. Lindemann, Über die Zahl π, *Math. Ann.*, **20** (1882), 213–225.

[16] J. Nagura, On the interval containing at least one prime number, *Proc. Japan Acad.*, **28** (1952), 177–181.

[17] Isaac Newton, *The method of fluxions and infinite series; with its application to the geometry of curve-lines*, Translated from Latin and published by John Colson, 1736.

[18] K. J. Nowak, Some elementary proofs of Puiseux's theorems, *Univ. Iagellonicae Acta Math.*, **38**, 279–282.

[19] W. Rudin, *Real and complex analysis. 3rd edition*, McGraw-Hill, 2nd printing, 1987.

[20] J. M. Ruiz, *The basic theory of power series*, Advanced Lect. in Math., Vieweg, 1993.

[21] V. A. Puiseux, Recherches sur les fonctions algébriques, *J. Math. Pures Appl.*, **15** (1850), 365–480.

[22] V. A. Puiseux, Recherches sur les fonctions algébriques, *J. Math. Pures Appl.*, **16** (1851), 228–240.

[23] http://en.wikipedia.org/wiki/Puiseux_series

[24] M. R. Spiegel, S. Lipschutz, J. J. Schiller and D. Spellman, *Complex Variables. 2nd. edition*, Schaum's Outline Series, McGraw-Hill, 2009.

[25] P. Schreiber, On the existence and constructibility of inscribed polygons, *Beiträge zur Algebra und Geometrie*, **34** (1993), 195–199.

[26] L. Rédei, *Algebra. I*, Akadémiai Kiadó, Budapest, 1954 (in Hungarian).

[27] P. L. Wantzel, Recherches sur les moyens de reconnaître si un Problème de Géométrie peut se résoudre avec le règle et le compas, *J. Math. Pures Appl.*, **2** (1837), 366–372.

[28] R. Wrede and M. R. Spiegel, *Theory and Problems of Advanced Calculus. 2nd edition*, Schaum's Outline Series, McGraw-Hill, 2002.

G. Czédli, University of Szeged, Bolyai Institute, Szeged, Aradi vértanúk tere 1, Hungary 6720; *e-mail*: czedli@math.u-szeged.hu; http://www.math.u-szeged.hu/~czedli/

Á. Kunos, University of Szeged, Bolyai Institute, Szeged, Aradi vértanúk tere 1, Hungary 6720; *e-mail*: akunos@math.u-szeged.hu; http://www.math.u-szeged.hu/~akunos/